DEN NORSKE KIRKE

Årsrapport 2024 for personvernombudet (PVO) i Den norske kirke

Hovedpunkter:

1. En høringsrunde i Den norske kirke viste at 84 % av respondentene ønsker å gjøre den felles ordningen for personvern og informasjonssikkerhet, som har eksistert siden 2022, til en forpliktende fellesordning.
2. I 2024 har PVO gitt skriftlig råd etter 167 henvendelser om personvern og informasjonssikkerhet fra ansatte og medlemmer. Dessuten har PVO besvart 29 muntlige henvendelser fra fellesråd og bispedømmer.
3. Etter et tilsyn med Den norske kirkes medlemsregister i 2024 konkluderte tilsynsgruppen - i likhet med i 2023 - at det er manglende lokal ajourføring av kirkelige handlinger, spesielt konfirmasjon. Manglende oppfølging fra Kirkerådets sekretariat, for eksempel i form av bindende pålegg fra den sentralt behandlingsansvarlige, innebærer manglende etterlevelse av medlemsregister-forskriften §§ 5, 10 og 12.
4. I 2024 var det god progresjon for kursing av nye medarbeidere innen personvern og informasjonssikkerhet. I læringsportalen tok ansatte modulene 1 - 4, mens det stoppet opp med modulene 5 - 7.
5. Ettersom personopplysninger sendes i e-post innen kirken, er det viktig at e-post ikke videresendes automatisk til usikre e-posttjenester. Det må utarbeides regler for videresending av e-post og bruk av private enheter i kirkens informasjonssystemer.

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 PVO 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

Alle kirkelige fellesråd har sluttet seg til Den norske kirkes felles ordning for personvern og informasjonssikkerhet, herunder felles personvernombud og

informasjonssikkerhetsansvarlig. En stillingsbeskrivelse for personvernombudet ble fastsatt av Kirkerådets direktør 1. oktober 2020[1]. Her fremgår det at PVO 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

I 2021 ble det ansatt en informasjonssikkerhetsansvarlig (CISO)[2][3]. CISO er en del av personvernteamet, som består av PVO, CISO og personvernjurist[4].

CISO er sekretær for Sikkerhetsutvalget for personvern og informasjonssikkerhet, som spiller en stadig større rolle i koordineringen av informasjonssikkerhetsarbeidet i hele trossamfunnet.

PVO holder regelmessige møter med CISO og sikkerhets- og beredskapsleder[5] for å sette personvernspørsmål inn i en større og helhetlig sikkerhetstenkning. Det foregår dessuten en omfattende kunnskapsutveksling med de andre nordiske kirkene, og med personvernombud i andre EØS-land.

En obligatorisk ordning for personvern og informasjonssikkerhet

Kirkerådet og fellesrådene utøver et felles behandlingsansvar for kirkens medlemsregister og noen felles informasjonssystemer. 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 behandlingsansvarlige, Kirkerådet og fellesrådene, avtaler sine respektive forpliktelser.

Kirkemøtet 2025 skal behandle en sak om regler om fellesordninger innen digitalisering, personvern og informasjonssikkerhet. I saken foreslås det at noen ordninger, som hittil har vært basert på en kontrakt mellom Kirkerådet og de kirkelige fellesrådene, gjøres til en del av kirkeordningen. Det gjelder blant annet digitaliseringsutvalget, sikkerhetsutvalget for personvern og informasjonssikkerhet og ordningen med et felles personvernombud. Dessuten foreslås det å regelfeste det felles behandlingsansvaret (PVF art 26) som i dag utøves av Kirkerådet og de kirkelige fellesrådene i tråd med dagens tilslutningsavtaler.

[1] https://kirken.no/globalassets/personvern/stillingsbeskrivelse_pvo.pdf
[2] Elsa Aaquist Storeng er ansatt i stillingen
[3] CISO betyr Chief Information Security Officer, en vanlig internasjonal betegnelse
[4] Guro Margrethe Mollnes fra juridisk avdeling i Kirkerådets sekretariat
[5] Svein Magne Christensen er ansatt i stillingen.

Som en del av saksforberedelsen ble det i 2024 gjennomført en høring blant lokale enheter i trossamfunnet Den norske kirke. Her ble alle kirkelige fellesråd og menighetsråd, kirkevergelaget, Hovedorganisasjonen KA og arbeidstaker–organisasjonene bedt om å svare.[6]

Det kom inn 109 høringssvar, inkludert 8 menighetsråd og 79 kirkelige fellesråd. Det er unison oppslutning om at kirken skal samle seg om digitale fellesløsninger (digitale verktøy). Mange mener at slike løsninger skal være frivillig/kontraktsbasert.

Spørsmål F i høringen lød: *Er du enig i at dagens fellesordning innen personvern og informasjonssikkerhet bør formaliseres som en forpliktende fellesordning?*

Her svarer 84 % (91 respondenter) ja, 10 % (11) nei og 6 % (7) vet ikke. Dette må ses som en solid støtte for den felles ordningen for personvern og informasjonssikkerhet som har eksistert siden 2022. For eksempel skriver Asker kirkelige fellesråd i sitt høringssvar:

> Dagens fellesordning innen personvern og informasjonssikkerhet er en svært god ordning, fordi den sikrer alle enhetene god kompetanse og kvalitet i arbeidet med personvern og informasjonssikkerhet.

Når PVO er rådgiver for ledelsen og "rapporterer til det øverste ledelsesnivå" er det i mange tilfeller kirkevergen. Holmestrand er et av kirkelige fellesrådene som går inn for at den felles ordningen for personvern og informasjonssikkerhet gjøres til en forpliktende fellesordning:

> I en verden der kravet til digitalt personvern og sikkerhet blir stadig mer viktig, vil det være behov for spesialkompetanse og regelverk som kan hjelpe oss alle til å ivareta dette feltet på en god og sikker måte.

Flere fellesråd peker på at de kirkelige fellesrådene ikke er direkte representert i Kirkemøtet eller i Kirkerådet, selv om alle kirkens valgte medlemmer kommer fra et sokn/fellesråd. Imidlertid er Kirkemøtet og Kirkerådet de eneste folkevalgte kirkelige organene som eksisterer på nasjonalt nivå. Samstyringsmodellen tilsier at digitaliseringsutvalget har representasjon fra hele virksomheten, også de kirkelige fellesrådene.

Grunnleggende rettigheter

Sommeren 2018 fikk EØS-landene en felles personvernlovgivning, personvernforordningen.[7] Det ble lovlig å behandle personopplysninger i hele EØS-området, og de registrerte sikres konfidensialitet, integritet og tilgjengelighet til informasjonssystemer. Lovgiveren ønsket at personvern og informasjonssikkerhet

[6] https://www.kirken.no/høringer
[7] https://lovdata.no/dokument/NL/lov/2018-06-15-38?q=personopplysningsloven

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 personverndom fra 2021 (den såkalte *Legelistesaken*) uttaler Høyesterett[8] at retten til personvern skal veies mot andre grunnleggende friheter som er sikret i Den europeiske unions pakt om grunnleggende rettigheter.[9].

Personvern og informasjonssikkerhet

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 betyr at den behandlingsansvarlige og databehandleren skal etablere et sikkerhetsnivå som skal gi «evne til å sikre vedvarende konfidensialitet, integritet, tilgjengelighet og robusthet i behandlingssystemene og -tjenestene.»

Siden 1. oktober 2018 har Den norske kirke ikke mottatt informasjon om relasjoner fra folkeregisteret fordi folkeregisterforskriften ble endret. Det er ingen tegn til at regjeringen ønsker å gi Den norske kirke samme lovhjemmel som for eksempel folkekirkene i Sverige, Finland og Danmark har.

- Personvernombudet noterer at Kirkerådets sekretariat fortsetter å minne regjeringen om dens forpliktelse til å levere relasjonsopplysninger fra folkeregisteret for at kirken skal kunne ha et ajourført medlemsregister.

Forslaget til Kirkemøtet innebærer at Kirkerådet skal utarbeide nye regler for hvordan Kirkerådet og de kirkelige fellesrådene utøver sitt felles behandlingsansvar i trossamfunnet Den norske kirke. Inntil nye regler foreligger, skjer arbeidet gjennom *Sikkerhetsutvalget for personvern og informasjonssikkerhet*[11]. Arbeidet er inntil videre basert på et mandat som Digitaliseringsstyret vedtok 16. desember 2022. Ifølge mandatet skal Sikkerhetsutvalget for personvern og informasjonssikkerhet:

- Utarbeide felles retningslinjer og gi råd i prinsipielle saker og valg i spørsmål knyttet til personvern og informasjonssikkerhet.
- Sørge for at oppdaterte retningslinjer og veiledningsmateriell er tilgjengelig.
- Sørge for å etablere master behandlingsprotokoll, bidra til at kirken har maler for behandlingsprotokoll samt bidra til at behandlingsansvarlige etablerer egen protokoll.
- Identifisere og initiere langsiktige tiltak med utgangspunkt i rapporterte risikovurderinger, hendelser og avvik.
- Initiere risikovurderinger, tester, analyser og tilsyn ved behov, og følge opp disse.
- Beslutte standardmal for databehandleravtale med vedlegg for felles løsninger.
- Etablere oversikt over og følge opp etterlevelsen av inngåtte databehandleravtaler.

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

[9] https://eur-lex.europa.eu/legal-content/DA/TXT/HTML/?uri=CELEX:12012P/TXT&from=EN

[11] *Sikkerhetsutvalget for personvern og informasjonssikkerhet* består av representanter for Kirkerådet, de kirkelige fellesrådene og Hovedorganisasjonen KA, arbeidsgiverorganisasjon for kirkelige virksomheter. Personvernombudet og CISO er også med i møtene, sistnevnte som utvalgets faste sekretær.

- Initiere og gjennomføre revisjon av leverandører som har inngått databehandleravtale/leverer felles løsning.
- Bidra til å heve kirkens kompetansenivå gjennom informasjon, opplæring og bevisstgjøring, slik at regelverket etterleves

PVO møter som fast rådgiver i Sikkerhetsutvalget. I 2024 har prioriterte arbeidsoppgaver i Sikkerhetsutvalget blant annet vært:

- Gjennomføre risikoanalyser og inntrengningstester av informasjonssystemer
- Sikre kirkens evne til håndtering av alvorlige uønskede hendelser
- Fortsette arbeidet med å oppdatere behandlingsprotokollen[12] for å gi oversikt over behandlingen av personopplysninger i forbindelse med de kirkelige handlingene (dåp, konfirmasjon, vielse og begravelse)
- Etablere et felles avvikssystem for trossamfunnet (som dekker brudd på personopplysningssikkerheten og informasjonssikkerheten)
- Innføre en felles standard for deling og synkronisering av kalendre i trossamfunnet

I 2024 vedtok sikkerhetsutvalget en strategi for informasjonssikkerhet og personvern for perioden 2025 - 2027. Målene for denne er å sikre

1. Helhetlig styring, sikkerhet og kontroll i hele trossamfunnet
2. Robust digital infrastruktur
3. Fellesløsninger og lik praksis
4. Evne til å håndtere hendelser og gjenetablere normal drift
5. Systematisk arbeid med kompetanse og kultur
6. Felles tilnærming til fysisk sikring

Blant virkemidlene for å nå disse målene er å:

- Etablere og formidle ledelsessystem for informasjonssikkerhet og personvern
- Forankre samstyringsmodell og felles ordning for informasjonssikkerhet og personvern i styrende organer
- Etablere rutiner for rapportering, oppfølging og kontroll

2. 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 (...)».

[12] Personvernforordningen fastsetter at de behandlingsansvarlige skal føre en protokoll over behandlingsaktiviteter som utføres under deres ansvar: https://lovdata.no/lov/2018-06-15-38/gdpr/a30

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:

- Hva må vi informere konfirmanter og foreldre om når de melder et medlem til konfirmasjon? Hvilke personopplysninger kan vi behandle?
- Har vi rett til å opplyse navnet til personer som har mottatt kirkelige handlinger i menighetsblad eller lokalavis?
- Kan vi invitere medlemmer eller andre til kirkelige arrangementer, for eksempel allehelgensgudstjeneste?
- Kan vi invitere kontaktpersonen fra en gravferd i Den norske kirke til en sorggruppe?

I 2024 har PVO gitt skriftlig råd etter 167 henvendelser om personvern og informasjonssikkerhet fra ansatte og medlemmer. Dessuten har PVO besvart 29 muntlige henvendelser fra fellesråd og bispedømmer.

PVO har deltatt i møtene i Sikkerhetsutvalget for personvern og informasjons–sikkerhet, i produkteierforum og i utrullingsrådet. PVO har i perioden deltatt i en rekke webinarer og workshops og deltatt i prostisamlinger i Østre Borgsyssel og i Øvre Romerike. Dessuten har PVO holdt en orientering for digitaliseringsstyret om Den norske kirkes ordning for personvern og informasjonssikkerhet.

Stillingen som PVO har vært fysisk plassert i digitaliseringsseksjonen og administrativt i administrasjonsavdelingen. I forbindelse med at det var planlagt opprettet en egen digitaliseringsavdeling, ble det foreslått at PVO og CISO burde være i den nye avdelingen. Et sentralt utsiktspunkt og nærhet til det øverste ledelsesnivået er nødvendig for å være oppmerksom på planlagte behandlinger av personopplysninger og kunne planlegge og drive personvernarbeidet.

Tilslutningsavtalene til kirkens felles ordning for personvern og informasjons-sikkerhet gjør at et økende antall kirkeverger henvender seg til PVO for å søke råd. Mange fellesråd fortsetter å behandle personopplysninger i usikret e-post. Det bør informeres bedre om muligheten til å sende og motta datafiler via sikre onlinetjenester, for eksempel *svarUT og eDialog*.

Den norske kirke fortsetter å anbefale Det europeiske personvernråds mal for databehandleravtale, som Den norske kirke har vært med på å oversette til norsk[13]. 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. Detaljene (tekniske og organisatoriske tiltak) ligger i vedleggene til databehandleravtalene.

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

Det er i 2024 etablert databehandleravtaler mellom Kirkerådet og Canva, samt oppdaterte databehandleravtaler med Vitec Agrando AS, Kirkedata AS og Kirkepartner AS. Det er i 2024 etablert en avtale om felles behandlingsansvar mellom Kirkerådet og Kniff Jobb AS, samt en avtale om felles behandlingsansvar mellom Asker kirkelige fellesråd og kommunalt NAV. Denne avtalen kan brukes som utgangspunkt for andre menigheter/fellesråd som trenger å behandle personopplysninger når de utfører tjenester for kommunen, for eksempel flyktningarbeid, barnehager eller eldreomsorg.

3. 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 CISO, internrevisor, sikkerhetsleder og juridisk avdeling i forbindelse med kontrollaktiviteter.

Tilsyn med medlemsregisteret våren/sommeren 2024

Det ble sammen med internrevisor og juridisk avdeling foretatt et tilsyn med Hamar og Nord-Hålogaland bispedømmer, 4 kirkelige fellesråd: Hammerfest, Alta, Hamar og Gran. Dessuten ble Tromsøysund menighet (ishavskatedralen) besøkt. Tilsynet ble gjennomført i to spor hhv. personvern/informasjonssikkerhet og sikkerhet. Tilsynsgruppen besto av personvernombudet, informasjonssikkerhetsansvarlig, konsulent fra medlemsregisterteamet, sikkerhetsleder og juridisk rådgiver.

Observasjoner og funn er på linje med foretatte tilsyn de siste årene. Mange kirkelige fellesråd melder at det er en utfordring å etterleve kravene til personvern og informasjonssikkerhet fordi de mangler ressurser og kapasitet. De er ofte henvist til å bruke kommunens IT-systemer isteden for informasjonssystemer som er beregnet for kirkelig virksomhet.

Formålet med tilsynet er å gi best mulig veiledning, støtte og føre kontroll med at reglene for personvern og informasjonssikkerhet følges i forvaltningen av medlemsregisteret. I 2024 ble sikkerhet tatt med som et tema i tilsynet.

- Konklusjoner for kirkelige fellesråd var at det er utfordringer knyttet til manglende ajourføring av kirkelige handlinger, spesielt konfirmasjon i medlemsregisteret. Kirkevergene har mottatt tilbakemelding og følger selv opp gitte råd.

- Konklusjoner for bispedømmene var at kontroll med føring av medlemsregister foretas i liten grad og at den fysiske sikkerheten kan være mangelfull. Konklusjon for Kirkerådets sekretariat var at det fremdeles er manglende etterlevelse av medlemsregisterforskriften §§ 5, 10 og 12. I forskriften pålegges Kirkerådet - den

sentralt behandlingsansvarlige - å sørge for at medlemsregisteret er ajour. For å sikre nødvendig konfidensialitet, integritet og tilgjengelighet, kan Kirkerådet gi lokal behandlingsansvarlig (fellesrådene) bindende pålegg. Denne muligheten har bare vært benyttet en enkelt gang. Veilednings- og kontrollprosesser er ikke tilfredsstillende etablert i forvaltningen.

IT-revisjon av informasjonssikkerhet og leverandørstyring

En IT-revisjon ble planlagt og gjennomført sommeren og høsten 2024 i regi av internrevisor og PwC.

Kirkedata og Vitec Agrando er to leverandører av fagsystemer som Den norske kirke er avhengig av for sin virksomhet. Disse systemene behandler personopplysninger og inneholder informasjonsverdier som er viktige for kirken å beskytte med tanke på konfidensialitet, integritet og tilgjengelighet. Kirken har som behandlingsansvarlig etter PVF artikkel 28 inngått databehandleravtaler med disse leverandørene. Avtalen forplikter behandlingsansvarlig til å føre regelmessig kontroll med at databehandleravtalen etterleves.

- I rapportens konklusjon blir samarbeidet med leverandørene beskrevet som godt og konstruktivt. Pwc påpeker at kirken har enkelte styrende dokumenter, men mangler et overordnet styringssystem for informasjonssikkerhet som sikrer enhetlig praksis i kirken. Pwc peker også på at det ikke er gjennomført overordnede risikovurderinger innen informasjonssikkerhet, og at det har begrenset innsikten i eksisterende risikoer og prioritering av tiltak.

4. Holdningsskapende tiltak

Læringsplattformen Educatia ble lansert sommeren 2022 og alle ansatte i rettssubjektet Den norske kirke ble opprettet som brukere i løpet av sommeren og høsten 2022. I 2022 hadde 98 ansatte i Kirkerådets sekretariat gjennomført fire kursmoduler i personvern og informasjonssikkerhet, hvilket var 80 prosent av de ansatte. I 2023 ble det fullført 63 kursmoduler i Kirkerådets sekretariat, hovedsakelig for nyansatte. De fire første modulene er obligatoriske, mens de tre siste er frivillige.

De fire første modulene er obligatorisk for ansatte i rettssubjektet Den norske kirke. Brukerstatistikken tyder på at mange medarbeidere faller av når det gjelder modulene 5 til 7.

I 2024 ble en rekke kirkelige fellesråd tatt inn i læringsplattformen. Nå har alle ansatte i Den norske kirke tilgang til læringsplattformen, forutsatt at kirkens Ansatt- og organisasjonsregister holdes oppdatert. Flere arbeidsgivere bør gjøre bruk av muligheten for å lage en liste over kurser som er nødvendige for ulike yrkeskategorier, for eksempel menighetssekretær, kirkeverge eller musiker.

5. Håndtering av avvik

Uønskede hendelser blir som regel meldt til personvernombudet via e-post eller telefon. Noen hendelser blir meldt via informasjonssikkerhetsansvarlig eller andre ansatte i Kirkerådets sekretariat.

Personvernombudet skaffer seg en oversikt over hva som er skjedd og gir råd til ledelsen om hvordan brudd på personopplysningssikkerheten skal håndteres. Dersom bruddet gjelder et kirkelig fellesråd, er det kirkevergen som mottar rådet og blir ansvarlig for oppfølgingen av det.

Etter hvert som kirken får flere felles informasjonssystemer, vil avvik ofte berøre mer enn ett kirkelig fellesråd, og oppfølgingen kan være kompleks og involvere mange fagpersoner innen Kirkerådets sekretariat, kirkelige fellesråd og databehandlere.

I 2024 ble det anskaffet et digitalt avvikssystem for hele trossamfunnet, som skal rulles ut i 2025. Ønsket er at det skal finnes ett, enkelt sted å melde avvik. En forhåndsbestemt arbeidsflyt skal sørge for at personvernombudet og informasjonssikkerhetsansvarlig blir orientert raskt nok og at de riktige fagpersonene blir involvert i oppfølgingen.

Avvik i Den norske kirke (meldt til Datatilsynet)

	2022	2023	2024
Kirkerådet	5 (2)	12 (5)	15 (4)
Fellesrådene	3 (3)	9 (7)	10 (4)
SUM	8 (5)	21 (12)	25 (8)

Det ble meldt 25 avvik i hele Den norske kirke i 2024. Av disse ble 8 meldt til Datatilsynet (tallene i parentes i tabellen over). Det har vært økning i melding av avvik, fra åtte meldte avvik i 2022 til 25 avvik i 2024. Avvikene som ikke er meldt av Kirkerådets sekretariat er meldt av kirkevergene i dialog med personvernombudet.

Økningen i meldte avvik tyder på en større bevissthet omkring personvern og informasjonssikkerhet, og en større aksept av at avvikshåndtering er et viktig ledd i organisasjonens kontinuerlige læring. Det er grunn til å tro at det er en underrapportering av avvik i trossamfunnet, noe som kan endre seg når det i 2025 etableres en felles rapportering og oppfølging av avvik i et elektronisk avvikssystem.

Avvik som kan trekkes frem fra 2024 er

- Teams-grupper har noen ganger manglende tilgangskontroll. Det kan ha oppstått fordi filbibliotek i Sharepoint er blitt opprettet som «offentlig» mens det er ment å være «privat». Når filbiblioteket gjøres tilgjengelig i Teams, tror administratoren at bare medlemmer av teamet kan se filbiblioteket. I virkeligheten kan alle ansatte se det fordi det er satt til «offentlig» i Sharepoint.

- Cyberangrep eller phishing rettet mot individer. Hackeren sender brev fra brukerens maskin og e-postadresse. Mottakerne tror henvendelsen er legitim.

- Foreldre har reservert seg mot at dåpsbarnets eller konfirmantens navn skal offentliggjøres. Menigheten publiserer allikevel navnet ved en feil.

- Lister over konfirmanter skal slettes når konfirmasjonen er over og handlingen er ført inn i medlemsregisteret. Noen menigheter har ikke sletterutiner og noen menigheter oppdaterer ikke medlemsregisteret.

I håndteringen av avvik er det avgjørende at det eksisterer logger som kan dokumentere hvem som har hatt tilgang til informasjonssystemene og hva de har hatt tilgang til. Dersom loggingen er for omfattende, vil den bli dyr, gjøre kartlegging vanskeligere og i seg selv utgjøre en sikkerhetsutfordring.

- Sikkerhetsutvalget bør utforme retningslinjer for logging som gjør det mulig for kirkens databehandlere å dokumentere sikkerhetshendelser i en rimelig periode. Samtidig må de slettes når formålet er oppfylt, slik at de registrertes rettigheter ivaretas.

6. Prioriteringer fremover

Som oppfølging av tidligere forvaltningsrevisjoner og tilsyn med medlemsregisteret, foreslår personvernombudet at følgende tiltak prioriteres i 2025:

- Etablere et ledelsessystem for informasjonssikkerhet og personvern, med dokumenterte rutiner og beredskapsplaner. Det legges vekt på å reetablere kritiske systemer etter hendelser.

- Etablere et årshjul for rapportering til ledergruppen i Kirkerådets sekretariat. Her flagges kommende saker og ledelsen beslutter et akseptabelt risikonivå for behandlingen av personopplysninger på forskjellige områder.

- Etablere regler for bruk av tjenesteutstyr og private enheter i kirkens informasjonssystemer.

- Veilede og hjelpe menigheter/fellesråd til å unngå å behandle person-opplysninger i e-post ved å gjøre tilgjengelig sikre kanaler for å sende og motta filer, for eksempel løsninger som *svarUT* og *eDialog*.

- Innføre regler for automatisk videresending av e-post til tjenester utenfor domenet kirken.no/kyrkja.no.

- Følge opp medlemsregisteret gjennom bindende pålegg når det oppdages manglende ajourføring av kirkelige handlinger. Utøve den styringsrett som medlemsregisterforskriften gir Kirkerådet i §§ 4, 5, 10 og 12.

- Utforme retningslinjer for logging som gjør det mulig for kirkens databehandlere å dokumentere sikkerhetshendelser i en rimelig periode.

Forøvrig, ut fra de henvendelsene personvernombudet har mottatt og de observasjonene som er gjort, ønsker PVO 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:

- Sette av ressurser som gjør det mulig for Sikkerhetsutvalget å følge opp tilslutningsavtalene. Det bør gjennomføres minst 3 personvernkonsekvens-vurderinger (DPIA'er) etter PVF art 35 i kritiske informasjonssystemer. Som mulige informasjonssystemer foreslår PVO medlemsregisteret, ANSORG og Læringsplattformen.

- Fortsette arbeidet med å flytte kirkelige fellesråd over fra kommunale IT-løsninger til informasjonssystemer som er egnet for kirkelig virksomhet

- Få arbeidsledere til å invitere og følge opp sine ansatte slik at det lages et anbefalt pensum for forskjellige medarbeidere i personvern og informasjonssikkerhet via læringsportalen Educatia

Oslo, 16. april 2025

Nils G. Indahl