DEN NORSKE KIRKE

Årsrapport 2025 for personvernombudet (PVO) i Den norske kirke

Hovedpunkter:

1. Siden 2022 har Den norske kirke hatt en felles ordning for personvern og informasjonssikkerhet basert på en tilslutningsavtale mellom Kirkerådet og de kirkelige fellesrådene. Kirkemøtet besluttet i 2025 at ordningen skal være en del av kirkeordningen.

2. I 2025 har PVO gitt skriftlig råd etter 172 henvendelser om personvern og informasjonssikkerhet fra ansatte og medlemmer. Dessuten har PVO besvart 22 muntlige henvendelser fra fellesråd og bispedømmer.

3. Den norske kirke opplever, i likhet med andre samfunnsinstitusjoner, en kraftig økning i cyberangrep, i særdeleshet phishingforsøk rettet mot kirkens ansatte. Angrepene blir stadig mer sofistikert og utføres av profesjonelle aktører og må forstås i en bredere geopolitisk kontekst, der digitale operasjoner brukes som virkemiddel for å skape uro og svekke tillit i åpne, demokratiske samfunn.

4. Sikkerhetsutvalget har vedtatt første versjon av Den norske kirkes beredskapsplaner for håndtering av cyberhendelser som påvirker digitale fellesløsninger. Beredskapsplanen bygger på kirkens overordnede risikovurdering innen informasjonssikkerhet og personvern, som ble gjennomført i 2025.

5. Det er fortsatt en varierende 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.

6. I 2025 var det god progresjon for kursing av nye medarbeidere innen personvern i Kirkerådet og i bispedømmene. Det er svært få av fellesrådene som ber sine ansatte om å ta kursene.

7. For å unngå bruk av utrygge tjenester, er det ønskelig at Den norske kirkes arbeidsgivere kan tilby KI-redskaper til sine medarbeidere. Det innebærer også en plikt for arbeidsgiveren til å gi medarbeideren de nødvendige arbeidsredskapene og opplæring i å bruke dem.

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

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] . CISO er en del av personvernteamet, som består av PVO, CISO og personvernjurist. Personvernombudet takker for et godt samarbeid med CISO, sikkerhetsrådgiver og juridisk seksjon.

En obligatorisk ordning for personvern og informasjonssikkerhet

I sitt møte 27. april 2025 fastsatte Kirkemøtet *Regler om fellesordninger innen digitalisering, personvern og informasjonssikkerhet i Den norske kirke.*

I § 5 (om *felles behandlingsansvar*) står det:

> Soknene og rettssubjektet Den norske kirke har felles behandlingsansvar, jf. personvernforordningen artikkel 26, i forbindelse med medlems- og publikumskontakt Den norske kirke har som trossamfunn. Kirkerådet gir nærmere regler om de behandlingsansvarliges respektive ansvar og roller.

[1] https://kirken.no/globalassets/personvern/stillingsbeskrivelse_pvo.pdf
[2] CISO er Chief Information Security Officer, et internasjonalt navn for informasjonssikkerhetsleder

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 (...)».

I *Regler om fellesordninger innen digitalisering, personvern og informasjonssikkerhet i Den norske kirke* § 4 står det:

> **Personvernombud**
> Den norske kirke har et felles personvernombud som ivaretar oppgaver etter personvernlovgivningen på vegne av alle kirkelige organer. Kirkerådet ansetter og har arbeidsgiveransvar for personvernombudet.

I § 2 fastsettes det at «Digitaliseringsutvalget organiserer og samordner felles digitaliseringsarbeid i Den norske kirke.» I § 3 fastsettes det at «Den norske kirkes sikkerhetsutvalg for personvern og informasjonssikkerhet (sikkerhetsutvalget) gir felles retningslinjer og råd om personvern og informasjonssikkerhet til kirkelige organer, og fører kontroll med at lovkrav på disse områdene blir fulgt.»

I sitt møte 2. februar 2026 fastsatte Kirkerådet nærmere regler for digitaliseringsutvalget og sikkerhetsutvalget. Digitaliseringsutvalget oppnevner medlemmer til sikkerhetsutvalget og vedtar dets budsjett. § 5 definerer sikkerhetsutvalgets oppgaver:

Sikkerhetsutvalget gir felles retningslinjer og råd om personvern og informasjonssikkerhet til alle kirkelige organer, og fører kontroll med at lovkrav på disse områdene blir fulgt.

Sikkerhetsutvalget skal

a) utvikle og forvalte felles strategi og ledelsessystem for informasjonssikkerhet og personvern i Den norske kirke

b) gi råd om konkrete krav til informasjonssikkerhet i digitale systemer i Den norske kirke, herunder hvordan personopplysninger skal håndteres i systemet

c) bidra til opplæring og veiledning av ansatte og frivillige i hele Den norske kirke innen informasjonssikkerhet og personvern

d) lage retningslinjer for rapportering og håndtering av avvik innen personvern og informasjonssikkerhet

e) påse at overordnede risiko- og sårbarhetsanalyser (ROS) gjennomføres og gjøres tilgjengelig for alle kirkelige organer, og gi råd om risikovurderinger kirkelige organer selv foretar

f) anbefale tiltak basert på rapporterte avvik og ROS-analyser

g) støtte ansvarlige i Den norske kirke i arbeid med databehandleravtaler

h) informere og involvere digitaliseringsutvalget, ledere og andre relevante personer om saker og tiltak på utvalgets område.

Sikkerhetsutvalget kan også

a) fastsette plan for kontroller med personvern og informasjonssikkerhetsarbeid i lokale, regionale og nasjonale kirkelige organer

b) i samarbeid med systemeier iverksette revisjoner overfor leverandører med fokus på informasjonssikkerhet og personvern.

I § 6 fastsettes det at «Kirkerådet skal sørge for at sikkerhetsutvalgets arbeid støttes med relevant kompetanse innen personvern og informasjonssikkerhet og ressurser for å følge opp utvalgets arbeid.»

CISO er sekretær for *sikkerhetsutvalget for personvern og informasjonssikkerhet*, som spiller en sentral rolle i koordineringen av informasjonssikkerhetsarbeidet i hele trossamfunnet.

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

Grunnleggende rettigheter

Sommeren 2018 fikk EØS-landene en felles personvernlovgivning, personvernforordningen.[3] 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 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[4] at retten til personvern skal veies mot andre grunnleggende friheter som er sikret i *Den europeiske unions pakt om grunnleggende rettigheter*.[4]

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.»

[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

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.

PVO møter som fast medlem i sikkerhetsutvalget. I 2025 har prioriterte arbeidsoppgaver i sikkerhetsutvalget blant annet vært:

- Gjennomføre risikoanalyser og inntrengningstester av informasjonssystemer
- Sikre kirkens evne til håndtering av alvorlige uønskede hendelser
- Etablere et felles avvikssystem for trossamfunnet (som dekker brudd på personopplysningssikkerheten og informasjonssikkerheten)

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, herunder digitale beredskapsplaner

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 (...)».

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:

- Kan vi bruke medlemsregisteret eller offentlige registre til å hente kontaktopplysninger når vi skal følge opp medlemmer?
- Har vi rett til å opplyse navnet til kommende konfirmanter i menighetsblad eller lokalavis?
- Kan vi invitere medlemmer eller andre til kirkelige arrangementer, for eksempel allehelgensgudstjeneste?

I 2025 har PVO gitt skriftlig råd etter 172 henvendelser om personvern og informasjonssikkerhet fra ansatte og medlemmer. Dessuten har PVO besvart 22 muntlige henvendelser fra fellesråd og bispedømmer.

PVO har deltatt i møtene i sikkerhetsutvalget for personvern og informasjons–sikkerhet, i produkteierforum og i utrullingsrådet.

Stillingen som PVO har vært fysisk og administrativt plassert i digitaliseringsavdelingen. Et sentralt utsiktspunkt og nærhet til det øverste ledelsesnivået er nødvendig for å være oppmerksom på planlagte behandlinger av personopplysninger og kunne planlegge og lede personvernarbeidet.

Kirkens felles ordning for personvern og informasjonssikkerhet 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.

Den norske kirke fortsetter å anbefale Det europeiske personvernråds mal for databehandleravtale, som Den norske kirke har vært med på å oversette til norsk[5]. 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 Det europeiske personvernråds mal som utgangspunkt. Detaljene (tekniske og organisatoriske tiltak) ligger i vedleggene til databehandleravtalene.

Det er i 2025 etablert databehandleravtaler mellom Kirkerådet og Adobe Systems, PBL Mentor og Kommuneforlaget. Den eksisterende databehandleravtalen med Kirkepartner AS er oppdatert.

Kontrollvirksomhet

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

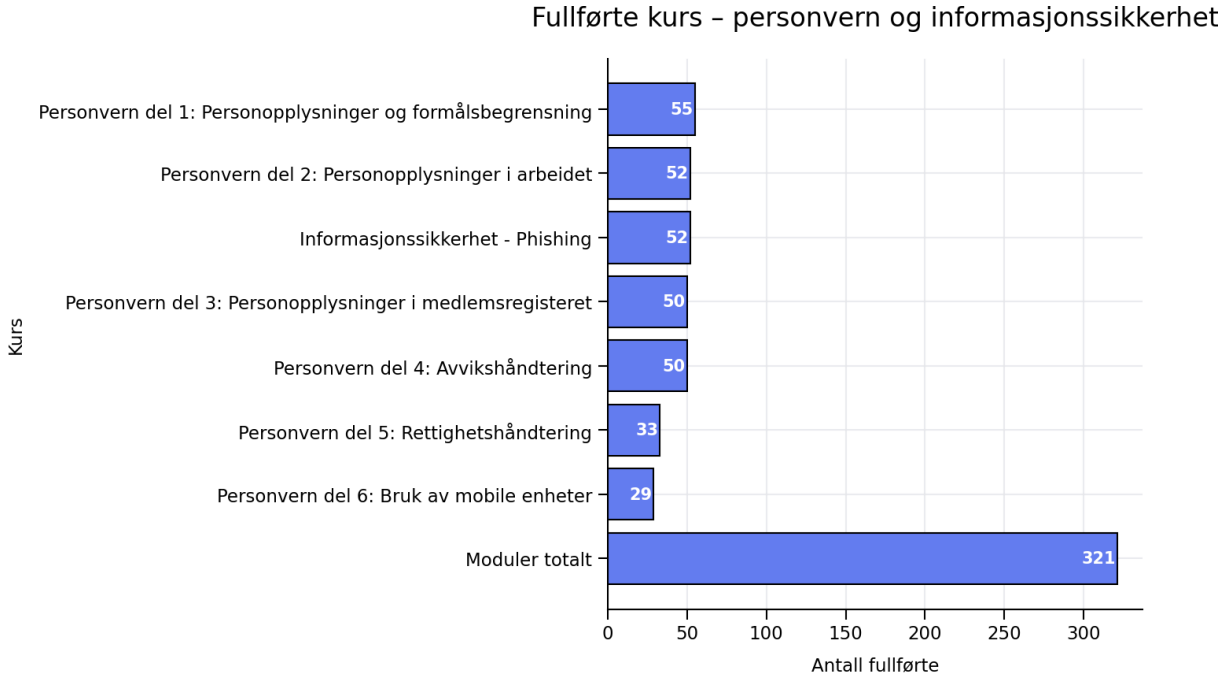
Personvernombudets annen oppgave er nevnt i PVF art 39 (1):

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,».

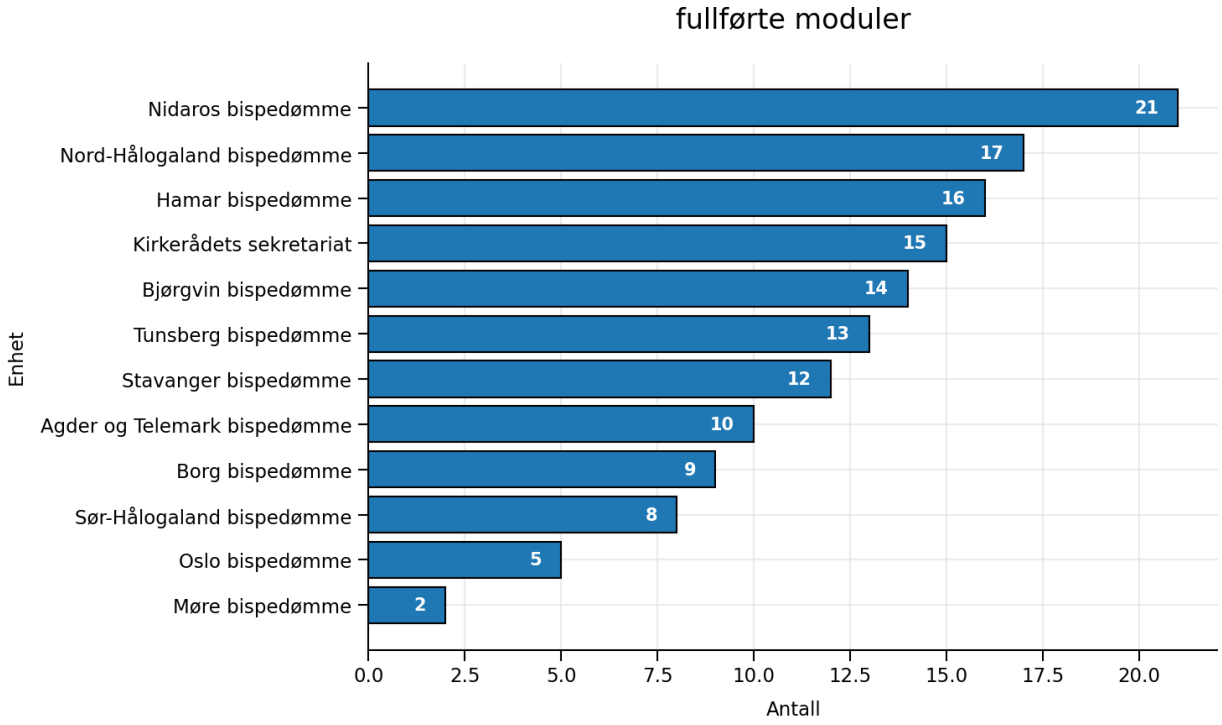
Tidligere ble det gjennomført årlige tilsyn med medlemsregisteret. Funnene var tildels de samme hvert år. Etter at stillingen som internrevisor ble lagt ned, gjennomføres internrevisjon ved hjelp av innleide ressurser. Det er viktig at tidligere observasjoner føres videre i de oppdragene Kirkerådet gir innleide ressurser..

3. Holdningsskapende tiltak

Læringsplattformen Educatia ble lansert sommeren 2022. Siden 2025 har alle ansatte i Den norske kirke tilgang til læringsplattformen. I 2025 ble det fullført 321 moduler i personvern og informasjonssikkerhet i læringsportalen. 52 ansatte gjennomførte kurs for å forhindre phishing-angrep.

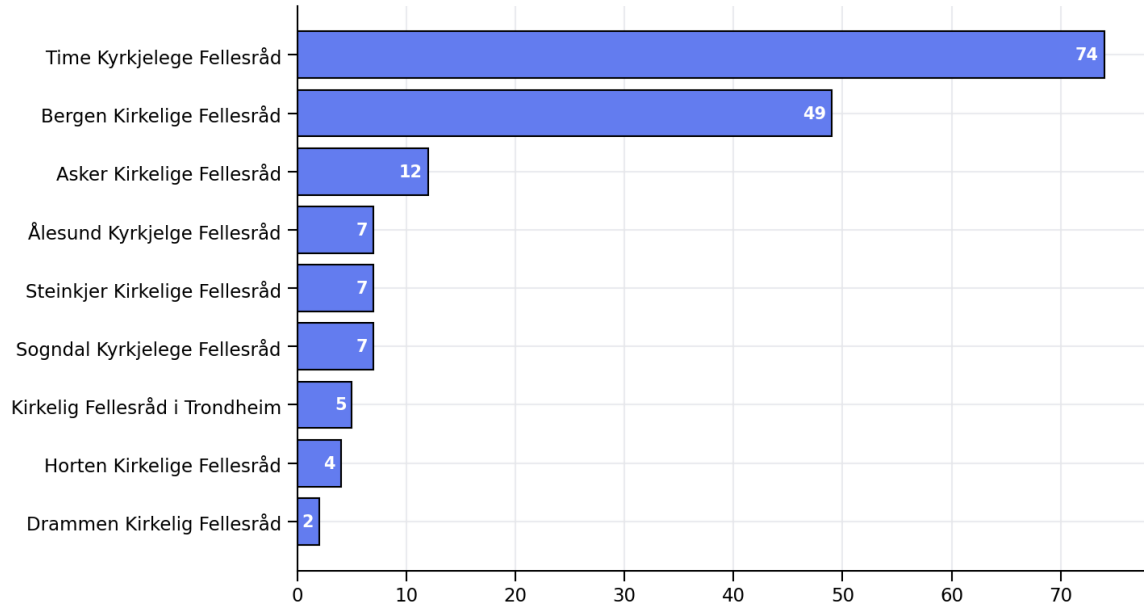


Det kan være behov for å gjenta kursene etter en periode. Antallet gjennomførte moduler fordelt på Kirkerådet og bispedømmene så slik ut i 2025:



Flere arbeidsgivere bør gjøre bruk av muligheten til å lage en profil med kurser som passer for ulike yrkeskategorier, for eksempel prest, menighetssekretær, kirkeverge eller musiker.

Svært få kirkelige fellesråd ber sine ansatte om å ta kurs i personvern og informasjonssikkerhet. Antallet gjennomførte moduler for de ni mest aktive fellesrådene ser slik ut i 2025:



4. 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.

Når et avvik er meldt, skaffer personvernombudet seg en oversikt over hva som er skjedd og gir råd til ledelsen om hvordan bruddet 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 skulle tas i full drift i 2026. Ønsket er at det 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	2025
Kirkerådet	5 (2)	12 (5)	15 (4)	25 (12)
Fellesrådene	3 (3)	9 (7)	10 (4)	11 (4)
SUM	8 (5)	21 (12)	25 (8)	36 (16)

Det ble meldt 36 avvik i Den norske kirke i 2025. Av disse ble 16 meldt til Datatilsynet (tallene i parentes i tabellen over). Det har vært en jevn økning i antall avvik, fra åtte meldte i 2022 til 36 i 2025. 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 2026 etableres en felles rapportering og oppfølging av avvik i et elektronisk avvikssystem.

Avvik som kan trekkes frem fra 2025 er

- Cyberangrep eller phishing rettet mot individer. Hackeren oppnår tilgang til den ansattes epost-konto og sender phishing-epost til den ansattes kontakter.. 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 synkroniserer ikke med 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. I håndteringen av mange avvik er det et problem at loggerutiner, herunder lagringstid, ikke er avklart på forhånd.

- Sikkerhetsutvalget er i prosess med å 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.

5. Bruk av kunstig intelligens i Den norske kirke

Høsten 2025 ble det gjennomført et pilotprosjekt for å teste bruk av kunstig intelligens (KI) i en begrenset prosjektgruppe sammensatt av brukere fra Kirkerådet, bispedømmene og enkelte kirkelige fellesråd. Tjenestene Copilot fra Microsoft og ChatGPT ble utprøvd.

En DPIA (Data Protection Impact Assessment), en vurdering av personvernkonsekvenser etter PVF art 35, ble gjennomført ved hjelp av en ekstern konsulent. Rapporten identifiserte 21 risikoer basert på erfaringene fra deltakerne i pilotgruppen.

Det viste seg at Copilot bruker alle dokumenter som ikke er klassifisert, selv om tjenesten begrenser seg til dokumenter som brukeren skal ha tilgang til. Brukeren må derfor klassifisere alle dokumenter som ikke skal brukes i KI. Klassifiseringen av dokumenter har vist seg å ha konsekvenser utover KI-piloten. Et dokument som er klassifisert vil ta med seg klassifiseringen over i andre informasjonssystemer, for eksempel det digitale arkivet Dnk 360.

Samtidig vurderer personvernombudet at det vil medføre en stor risiko dersom Den norske kirke ikke tilbyr KI-redskaper til sine medarbeidere. Erfaringen tilsier at medarbeiderne ellers vil bruke forbrukerprodukter - det vi kan kalle skygge-IT - hvor arbeidsgiveren har begrenset kontroll med hvilke dokumenter som blir delt med KI-tjenester.

- Ut fra en helhetsvurdering er det ønskelig at Den norske kirkes ulike arbeidsgivere kan tilby KI-redskaper på en trygg måte til sine medarbeidere. Det ligger i dette også en plikt for arbeidsgiveren til å gi medarbeideren de

nødvendige arbeidsredskapene og gi ham/henne den nødvendige opplæringen.

- Felles for de gjenværende, identifiserte risikoene er at de kan reduseres ved pilotering, testing, bevisstgjøring, retningslinjer, opplæring og menneskelig kontroll. Den enkelte medarbeider må lære å klassifisere riktig og forholde seg kritisk til KI-resultater.

6. Prioriteringer fremover

Som oppfølging av tidligere forvaltningsrevisjoner og tilsyn med medlemsregisteret, foreslår personvernombudet at følgende tiltak prioriteres i 2026:

- Etablere et ledelsessystem for informasjonssikkerhet og personvern, med prinsipper, dokumenterte rutiner og beredskapsplaner. I beredskapsplanverket legges det 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. Innføre regler for bruk av privat e-post i jobbsammenheng, samt for automatisk videresending av e-post til eksterne e-posttjenester, som f.eks. 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.

- Veilede og hjelpe menigheter/fellesråd i bruk av KI-tjenester og tilby kurser til medarbeiderne.

For øvrig, 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 det regelverket som er fastsatt av Kirkemøtet. Det bør gjennomføres minst 3 personvernkonsekvensvurderinger (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 og andre eksterne IT-tjenester til tjenester som er egnet for kirkelig virksomhet

- Oppmuntre arbeidsledere i menighetene til å invitere og følge opp sine ansatte slik at medarbeiderne pålegges å ta kurser i personvern og informasjonssikkerhet via læringsportalen Educatia

Oslo, 1. april 2026

Nils G. Indahl