Retningslinjer for personvern

Sist oppdatert: 18.04.2024

Innhold

Innledning 2
Begreper 2
Personvern 2
Personvernforordningen/GDPR 2
Personopplysningsloven 2
Hva er personopplysninger? 2
Sensitive personopplysninger 3
Behandle personopplysninger 3
Personvernprinsippene 3
Hvordan kan du som tillitsvalgt bidra til et godt personvern? 4
Ulike problemstillinger 4
Medlemslister og medlemsdata 4
Kan man sende medlemslister på e-post? 4
Kan man motta medlemslister på e-post? 4
Hvordan sende e-post til medlemmene 5
Sikker overføring av filer på Min side 5
Bruk av kunstig intelligens (KI) 5
Er NN medlem av PF? 6
Kan man bruke reelle eksempler i opplæringen av tillitsvalgte? 6
Deling på nett (sosiale medier) 6
Elektroniske dokumenter 6
Slik passordbeskytter du en Excel-fil 7
Slik passordbeskytter du en PDF-fil 7
Slik passordbeskytter du med 7-Zip 8
Hvis opplysninger havner på avveie eller du oppdager brudd på personvern 8
Kilder 9

Innledning

Politiets Fellesforbund (PF) må sikre at tillitsvalgte på alle nivå, og andre som har tilgang på medlemsopplysninger, har god kunnskap om håndtering av personopplysninger og bidrar til en god etterlevelse av bestemmelsene i personvernlovgivningen. Denne veiledningen sikter på å gi deg som tillitsvalgt den kunnskapen du trenger for å håndtere personvern i fagforeningshverdagen.

Begreper

Personvern

Personvern handler om retten til et privatliv og retten til å bestemme over egne personopplysninger. Denne retten er beskyttet av både Den europeiske menneskerettskonvensjonen (EMK) og den norske Grunnloven.

Personvernforordningen/GDPR

EUs forordning for personvern, også kjent som **General Data Protection Regulation (GDPR)**, utgjør sammen med deler av personopplysningsloven, et omfattende regelsett som gjelder for alle EU/EØS-land. GDPR setter standarden for behandling av personopplysninger og ivaretakelse av personvernet.

Personopplysningsloven

Dette er en norsk lov med formål å beskytte den enkelte mot at personvernet blir krenket gjennom behandling av personopplysninger. Loven gjennomfører GDPR i norsk rett. Forordningen er dermed en del av personopplysningsloven og gjelder som norsk lov.

Hva er personopplysninger?

Personopplysninger er alle opplysninger og vurderinger som kan knyttes til deg som enkeltperson. Typiske eksempler på personopplysninger er navn, adresse, telefonnummer, e-postadresse, og fødselsnummer.

Videre inkluderer personopplysninger identifikatorer som, når de kombineres, kan identifisere en person. Dette kan være en ikke navngitt person som likevel kan identifiseres gjennom opplysninger om lokalisering, arbeidsstatus, alder, og lignende.

All bruk av personopplysninger må ha et behandlingsgrunnlag, et rettslig grunnlag, for å være lov.

Sensitive personopplysninger

Sensitive personopplysninger er personopplysninger som har strengere krav til behandling enn andre personopplysninger.

Fagforeningstilhørighet betraktes som en sensitiv opplysning, i likhet med opplysninger om etnisitet, religionstilhørighet og helseopplysninger, for å nevne noen eksempler.

Som hovedregel er det forbudt å behandle slike opplysninger, men det finnes unntak. For fagforeninger er unntak spesifikt beskrevet i **Personvernsforordningen (GDPR) Artikkel 9, Behandling av særlige kategorier av personopplysninger, punkt 2d.**

Det er likevel viktig at vi behandler personopplysningene om våre medlemmer med stor forsiktighet.

Artikkel 9.Behandling av særlige kategorier av personopplysninger

2 d. Behandlingen utføres av en stiftelse, sammenslutning eller et annet ideelt organ hvis mål er av politisk, religiøs eller fagforeningsmessig art, som ledd i organets berettigede aktiviteter og med nødvendige garantier, forutsatt at behandlingen bare gjelder organets medlemmer eller tidligere medlemmer eller personer som på grunn av organets mål har regelmessig kontakt med det, og at personopplysningene ikke utleveres til andre enn nevnte organ uten de registrertes samtykke.

Behandle personopplysninger

Behandling av personopplysninger omfatter enhver bruk og alle typer handlinger med personopplysninger, inkludert innsamling, lagring, bruk, deling og sletting. Disse aktivitetene kan utføres både manuelt og automatisk.

Politiets Fellesforbund er behandlingsansvarlig for medlemmenes personopplysninger. Den behandlingsansvarlige har det overordnede ansvaret for å sikre at behandlingen av personopplysninger overholder personvernprinsippene og det gjeldende regelverket.

Vårt formål med behandlingen (behandlingsgrunnlaget) er å oppfylle forpliktelsene vi har for å sikre våre medlemmers rettigheter, i samsvar med vedtektene og tariffavtalene som vi har inngått med medlemmenes arbeidsgivere og deres arbeidsgiverorganisasjoner.

Formål og virksomhet står beskrevet i vedtektene, spesifikt i § 1-2 Formål, § 1-3 Forbundets virksomhet, og § 3-1 Opptak av enkeltmedlemmer.

Personvernprinsippene

Alle som behandler personopplysninger, må opptre i samsvar med personvernprinsippene. Disse prinsippene er utformet for å sikre at behandlingen av personopplysninger skjer på en måte som i ivaretar forutsigbarhet og forholdsmessighet for den enkelte:

- **Lovlighet, rettferdighet og åpenhet**: Behandlingen skal være lovlig, rettferdig og oversiktlig for den registrerte.
- **Formålsbegrensning:** Personopplysninger skal kun behandles for spesifikke, uttrykkelig angitte og legitime formål.
- **Dataminimering:** Mengden personopplysninger som samles inn og behandles, skal begrenses til det som er nødvendig for å nå formålet med behandlingen.
- **Riktighet:** Personopplysninger skal være korrekte og, om nødvendig, oppdaterte.

- **Lagringsbegrensning:** Personopplysninger skal slettes eller anonymiseres når de ikke lenger er nødvendige for formålet de ble samlet inn for.
- **Integritet og konfidensialitet:** Personopplysninger skal behandles på en måte som sikrer tilstrekkelig sikkerhet, inkludert beskyttelse mot uautorisert eller ulovlig behandling og mot utilsiktet tap, ødeleggelse eller skade.
- **Ansvarlighet:** Den behandlingsansvarlige er ansvarlig for å opptre i samsvar med reglene for behandling av personopplysninger.

Hvordan kan du som tillitsvalgt bidra til et godt personvern?

Som tillitsvalgt kan du få tilgang til personopplysninger og er forpliktet til å behandle disse opplysningene i samsvar med formålet til Politiets Fellesforbund.

Behandling av personopplysninger, spesielt opplysninger om fagforeningsmedlemskap, er underlagt strenge regler. Disse opplysningene skal alltid behandles med stor forsiktighet.

Som tillitsvalgt skal du:

- **Innhente og oppbevare kun den informasjonen som er nødvendig** for å oppfylle formålet.
- **Sikre at personopplysninger oppbevares trygt,** for å forhindre uautorisert tilgang, endring eller tap.
- **Påse at personopplysninger slettes eller makuleres** når formålet er oppfylt, og det ikke lenger er nødvendig å oppbevare opplysningene.

Ulike problemstillinger

Medlemslister og medlemsdata

Hovedtillitsvalgte i lokallagene (leder, nestleder, organisasjonssekretær m.fl.) og ansatte på forbundskontoret, har tilgang til medlemsdata gjennom pålogging på *Min side*. Tilgangen er begrenset til medlemmer i eget lokallag (forbundskontoret har ikke denne begrensningen). Tillitsvalgte på lavere nivå kan kommunisere via SMS og e-post gjennom en kommunikasjons-kanal på *Min side*. Tilgangen er begrenset til medlemmer i egen enhet. Tilgangsstyring styres av verv, som ajourføres av lokallaget selv.

Kan man sende medlemslister på e-post?

Personopplysninger skal ikke distribueres videre uten at det er strengt nødvendig for utøvelsen av rollen som tillitsvalgt eller ansatt på forbundskontoret.

Medlemslister kan sendes på e-post, forutsatt at ekstra sikkerhetstiltak følges. Den enkleste måten å sikre dokumentet på, er å sette passord på det (kryptere dokumentet). Ikke glem passordet du har satt, ellers får hverken du eller mottakeren åpnet fila. Husk å alltid benytte en separat kommunikasjonskanal (for eksempel SMS) for passord til mottakeren.

Kan man motta medlemslister på e-post?

Vurder alltid nødvendigheten av å motta personopplysninger. Hvis det er nødvendig, avtal en sikker overføringsmetode, for eksempel ved å sette passord på filen.

Hvis du mottar medlemslister på e-post uten passordbeskyttelse, informer avsenderen om at dette ikke er en sikker metode for sending av personopplysninger. Gi beskjed om at fremtidige henvendelser må ivareta sikkerhet og personvern.

Hvordan sende e-post til medlemmene

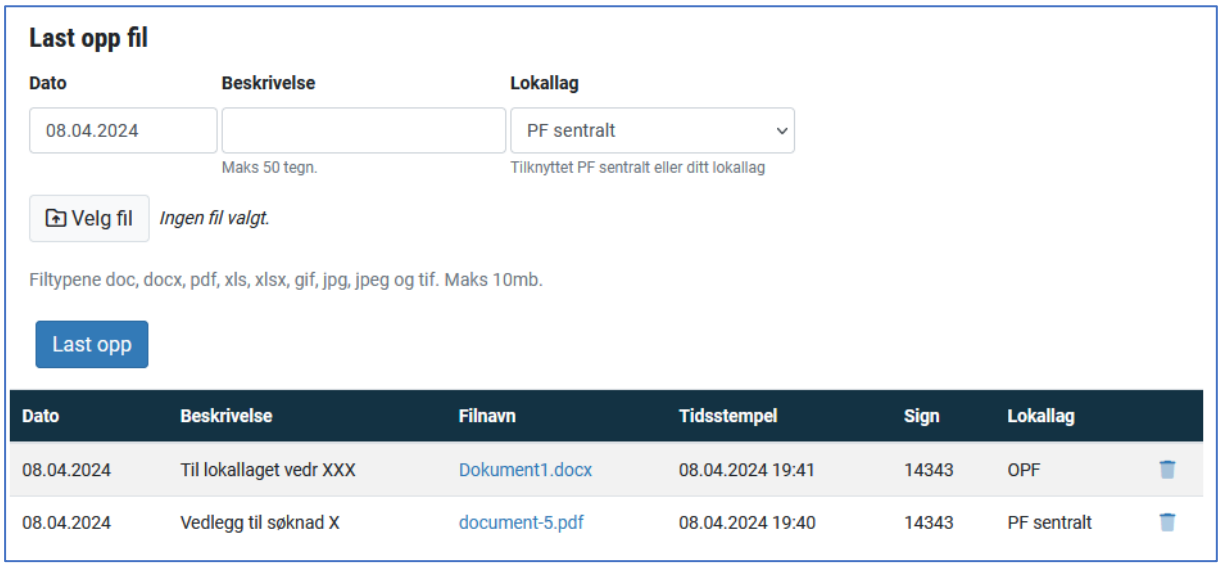
Masseutsendelser av e-post til medlemmene bør primært gjøres via kommunikasjonsfunksjonen på *Min side.* Der er personvernet ivaretatt av den tekniske løsningen og mottakerne ikke ser hverandres e-postadresser.

Ved e-postutsendelse via et e-postprogram (for eksempel Outlook):

- Hvis mottakergruppen ikke kjenner hverandre og der e-postadressene skal holdes private, bruk blindkopi-feltet. Eksempel: deler av medlemsmassen.
- Hvis alle mottakerne allerede kjenner hverandre og er komfortable med at deres e-postadresser deles, kan det være akseptabelt å bruke det vanlige «til»-feltet. Eksempel: lokallageledergruppen, forbundsstyret etc.
- Hvis mottakergruppen skal ha dialog eller samarbeid, bruk det vanlige «til»-feltet. Eksempel: lokale likestillingskontakter, prosjektgrupper etc.

Sikker overføring av filer på Min side

For behovet med å dele dokumentasjon som inneholder personopplysninger eller sensitive personopplysninger fra medlem til lokallaget eller PF sentralt, tilbyr *Min side* funksjonalitet for dette. Under *Medlem / Mine filer*, kan medlemmer laste opp filer enten til PF sentralt eller til lokallaget. Dette kan være for eksempel dokumentasjon for innvilget stipend. Medlem som laster opp fil(er) må varsle mottaker om at filen er lastet opp, det finnes per nå ingen automatisk varsling på dette.



Bruk av kunstig intelligens (KI)

KI kan være et nyttig verktøy i arbeidshverdagen. Det er mulig å benytte seg av gratis tilgjengelig KI-verktøy, som for eksempel Copilot i Edge eller ChatGPT. Når du bruker slike verktøy, er det imidlertid viktig å huske på ikke å dele sensitiv bedriftsdata, personopplysninger, eller informasjon som samlet kan identifisere en person.

Er NN medlem av PF?

Som tillitsvalgt kan du oppleve å få spørsmål fra eksterne parter om en bestemt person er fagorganisert hos oss. Selv om det kan være fristende å svare bekreftende og stolt, er det viktig å huske på at:

- Nei, du kan ikke dele denne informasjonen. Fagforeningstilhørighet er en sensitiv personopplysning og skal ikke deles med mindre mottakeren har en legitim grunn til å vite dette.
- En legitim grunn kan være at en arbeidsgiver trenger informasjonen for å kunne igangsette trekk eller for å oppfylle andre kollektive avtaler som er knyttet til fagforeningstilhørigheten, for eksempel i forbindelse med fagforeningsrepresentasjon eller under lønnsforhandlinger.

Vurder alltid hva som er formålet til den som spør.

Kan man bruke reelle eksempler i opplæringen av tillitsvalgte?

Når du bruker eksempler fra arbeidsplassen eller etaten i for eksempel opplæring, er det viktig å vurdere hvilke personopplysninger du inkluderer.

- Hvilke opplysninger er nødvendig for formålet med eksemplet? Husk at personopplysninger inkluderer identifikatorer som, når de kombineres, kan identifisere en person.
- Eksempel: Istedenfor å si «jeg hadde en sak med en nivå-2 leder i Innlandet», kan du omformulere til «jeg hadde en sak med en nivå-2 leder i et politidistrikt» for å unngå mulig identifisering.

Deling på nett (sosiale medier)

Et bilde er en personopplysning dersom personen kan gjenkjennes.

- **Samtykke ved deling av informasjon:** Før du deler personopplysninger eller bilder av medlemmer på sosiale medier (inkludert i lukkede grupper), må du sikre at du har innhentet et informert og frivillig samtykke fra de involverte. Medlemmene bør være fullt informert om hvilken informasjon som deles og hvordan den vil bli brukt.
- **Vurdering av kontekst ved bildebruk:** Selv om noen bilder kan deles offentlig, for eksempel fra en offentlig begivenhet, uten eksplisitt samtykke, er det viktig å alltid vurdere om delingen respekterer den avbildedes privatliv og rettigheter.

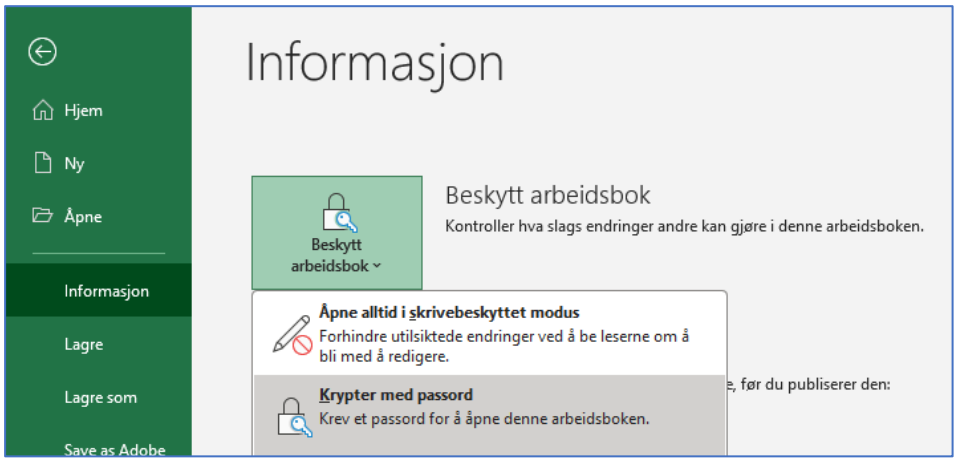
Elektroniske dokumenter

Elektronisk lagring av dokumenter skal kun foretas når det er et faktisk behov, og lagringen skal kun vare så lenge dette behovet eksisterer. Informasjonen skal slettes når formålet med behandlingen er oppfylt.

Personopplysninger om medlemmer skal lagres på medier som er sikret med kryptering eller passord, for å forhindre at arbeidsgiver eller andre uvedkommende får tilgang.

Slik passordbeskytter du en Excel-fil

- Åpne **Fil**-menyen.
- Velg **Informasjon**.
- Velg **Beskytt arbeidsbok**.
- Velg **Krypter med passord**.



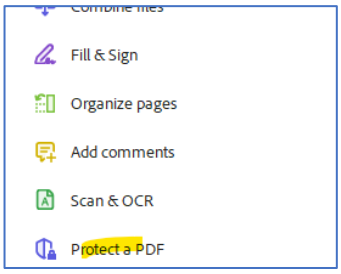
Du fjerner passordbeskyttelsen på tilsvarende måte (forutsatt at du har det lagret på et sikkert sted). Slett passordet som er lagt inn og velg **OK**.

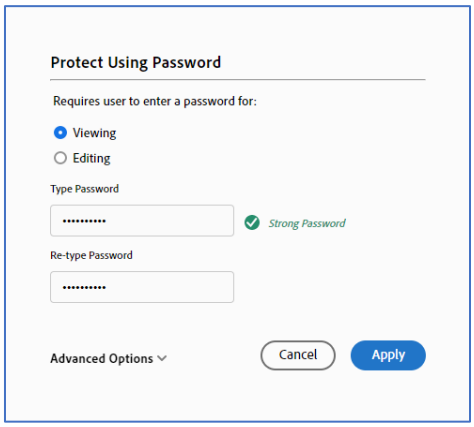
Slik passordbeskytter du en PDF-fil

For å sette passordbeskyttelse på en PDF-fil, kreves det en Adobe-lisens (Standard eller Pro). Denne funksjonaliteten er ikke tilgjengelig i gratisversjon av Adobe. Se neste punkt for alternativ metode, om du ikke har tilgang på Adobe Standard eller Pro.

Med Adobe Pro:

- Velg **All tools**.
- Velg **Protect a PDF**.
- Velg **Protect with password**.
- Sett et sterkt passord og klikk **Apply**.



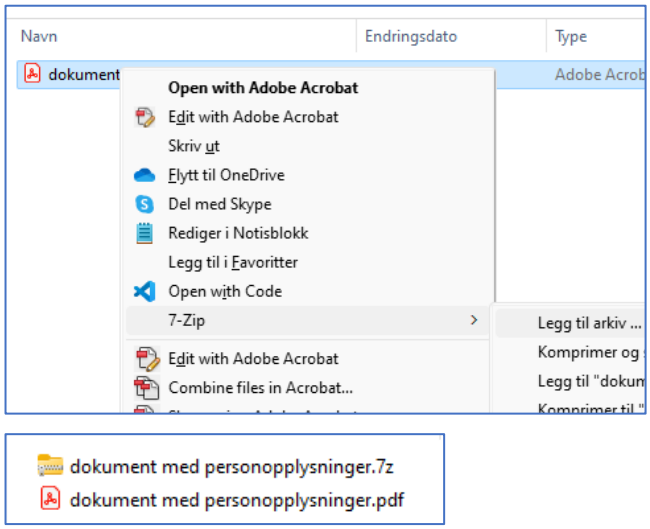


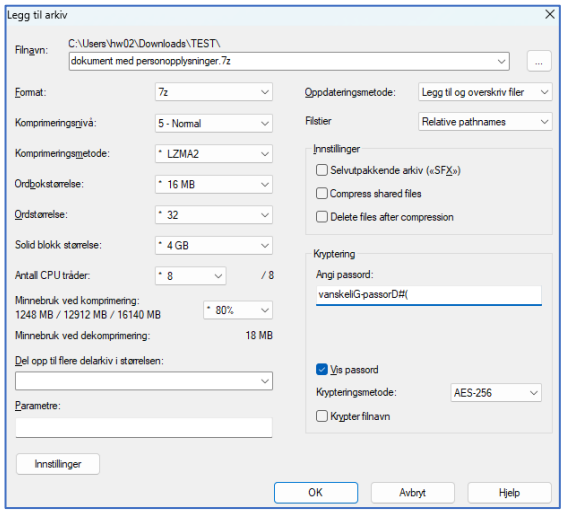
Slik passordbeskytter du med 7-Zip

7-Zip er en gratis programvare med åpen kildekode som kan brukes til å komprimere og passordbeskytte filer og mapper. Programvaren kan lastes ned fra: https://7-zip.org/

For å passordbeskytte en fil med 7-zip:

- Høyreklikk på filen du ønsker å beskytte.
- Velg **7-Zip** og deretter **Legg til arkiv (Add to Archive)**.
    - Hvis valget ikke vises, klikk på **Vis flere alternativer** (nederste valg) for å få det til å dukke opp.
- Skriv inn et filnavn og passord, deretter klikk **OK**.





Hvis opplysninger havner på avveie eller du oppdager brudd på personvern

Det er viktig å melde fra om avvik for å sikre et godt personvern og for å lære av eventuelle feil. Eksempler på avvik inkluderer:

- Sensitive personopplysninger som har kommet på avveie (for eksempel medlemslister).
- E-post med personopplysninger sendt til feil mottaker.
- Angrep mot datasystemer (hacking) som har resultert i at personopplysninger er blitt hentet ut, endret, eller gjort utilgjengelige.
- Manglende eller feilaktig tilgangsstyring som har tillatt uvedkommende tilgang til personopplysninger.
- Oppdagelse av sikkerhetshull som mulig har blitt utnyttet av uvedkommende. Uautorisert eller utilsiktet publisering av personopplysninger som ikke skulle ha vært offentliggjort, eller som ikke har blitt tilstrekkelig anonymisert.
- Dokumenter som skulle vært makulert, men som er kastet.
- Mistet, gjenglemt, eller stjålet utstyr (for eksempel PCer, minnepinner ikke kryptert) som inneholder personopplysninger.

Brudd på personvern meldes til Politiets Fellesforbund på personvern@pf.no. Du kan også ta kontakt ved spørsmål eller behov for ytterligere veiledning.

Kilder

- Personopplysningsloven: https://lovdata.no/dokument/NL/lov/2018-06-15-38
- Personvernforordningens Artikkel 6, *Behandlingens lovlighet*: https://lovdata.no/dokument/NL/lov/2018-06-15-38/KAPITTEL_gdpr-2#gdpr/a6
- Personvernforordningens Artikkel 9, *Behandling av særlige kategorier av personopplysninger*: https://lovdata.no/lov/2018-06-15-38/gdpr/a9
- Politiets Fellesforbunds personvernerklæring: https://pf.no/page/personvernerklaering
- Politiets Fellesforbund vedtekter: https://pf.no/temaomrader/vedtekter
- Datatilsynet: https://www.datatilsynet.no/
- Store norske leksikon: https://snl.no/personopplysningsloven