*Forslag til MAL 1*

**STYRINGSSYSTEM /RUTINER**

**FOR**

**INFORMASJONSSIKKERHET**

**[AVDELING XX]**

[](https://www.google.no/url?sa=i&rct=j&q=&esrc=s&source=images&cd=&cad=rja&uact=8&ved=0ahUKEwiN7dfvnuXTAhUEBywKHRxjD5AQjRwIBw&url=https://www.kreftregisteret.no/Generelt/Om-Kreftregisteret/Personvern/Informasjonssikkerhet-og-personvern/&psig=AFQjCNEC7_Cmrri8zcivRp0cS421rml5dg&ust=1494502698106552)

Innhold

1. Bakgrunn 3

1.1. Innledning 3

1.2. Formål 3

2. Ord og uttrykk 3

3. sikkerhetsMÅL 5

4. Roller og ansvar FOR informasjonssikkerhet 5

4.1. Avdelingsleder 5

4.2. Behandlingsansvarlig 5

4.3. Sikkerhetsansvarlig 6

4.4. øvrige ansatte og tillitsvalgte 6

5. OVERSIKT OVER BEHANDLING AV PERSONOPPLYSNINGER 7

6. RUTINER 8

6.1 Avdelingsstyrets gjennomgang 8

6.2 risikovurdering 8

6.3 Retten til innsyn, retting og sletting 8

6.4 Personvernerklæring 9

6.5 Inngåelse av databehandleravtaler 9

6.6 Avviksbehandling 9

6.7 Overføring av personopplysninger 9

6.8 Opplæring (Sikkerhet) 9

7. Vedlegg 10

# 

# Bakgrunn

## Innledning

Personopplysningsloven (POL) setter krav til at virksomheter som behandler personopplysninger skal etablere et styringssystem for informasjonssikkerhet. Dette dokumentet er utarbeidet for å dekke kravene til et slikt system.

Personopplysningsloven består av nasjonale regler og EUs personvernforordning (også kalt *GDPR* - General Data Protection Regulation). Forordningen er et sett regler som gjelder for alle EU/EØS-land. Sammen med særlovgivning om personvern på enkelte områder, utgjør dette personvernregelverket.

[Avdeling xx] behandler personopplysninger om medlemmer og egne ansatte. Avdelingen innhenter personopplysningene for å kunne utøve sin virksomhet.

Dokumentet inneholder overordnede føringer for informasjonssikkerhet, roller og ansvar, samt kontrollerende rutiner.

## Formål

Formålet med styringssystemet er å sette mål og føringer for informasjonssikkerhetsarbeidet knyttet til forbundets behandlinger av personopplysninger.

# Ord og uttrykk

| **Emne** | **Definisjon** |
| --- | --- |
| Behandling av personopplysninger | Enhver bruk av personopplysninger, som for eksempel innsamling, registrering, sammenstilling, lagring og utlevering eller en kombinasjon av slike bruksmåter.  (Jf. POF Artikkel 5) |
| Behandlingsansvarlig | Den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes.  (Jf. POF Artikkel 4, punkt 7) |
| Databehandler | En juridisk enhet som behandler personopplysninger på vegne av den behandlingsansvarlige.  Enheten er en ekstern virksomhet i forhold til avdelingen. (Jf. POF Artikkel 28 og 29) |
| Informasjonssystemet | Samlebetegnelse på alt utstyr, systemer og nettverks­komponenter som inngår i IT-løsning. |
| Integritet | Å sikre at informasjonen og behandlingsmetodene er nøyaktige og fullstendige.  (Jf. POF Artikkel 5) |
| Kompromittering | Brudd på konfidensialitet, tilgjengelighet eller integritet.  (Jf. POF Artikkel 5) |
| Konfidensialitet | Å sikre at informasjonen er tilgjengelig bare for dem som har autorisert tilgang.  (Jf. POF Artikkel 5) |
| Personopplysninger | Opplysninger og vurderinger som kan knyttes til en enkeltperson.  (Jf. POF Artikkel 4, pkt. 1) |
| Personopplysningsloven (POL) | Lov om behandling av personopplysninger, 15. juni 2018, nr. 38. Rettet 02.09.2021. |
| Personopplysningsforordningen (POF) | [EØS-avtalen vedlegg XI](https://lovdata.no/avtale/avt-1992-05-02-1-v11) nr. 5e (forordning [(EU) 2016/679](https://lovdata.no/eu/32016r0679)) om vern av fysiske personer i forbindelse med behandling av personopplysninger |
| Sensitive personopplysninger | Opplysninger om:   * rasemessig eller etnisk opprinnelse * politisk oppfatning * religion * filosofisk overbevisning * fagforeningsmedlemskap[[1]](#footnote-1) * genetikk og biometrikk med det formål entydig å identifisere noen * helseopplysninger * seksuelle forhold eller seksuell orientering   (Jf. POF Artikkel 9) |
| Sikkerhetshendelse | En hendelse som får konsekvenser for informasjons­sikkerheten i virksomheten. |
| Sikkerhetstiltak | Et administrativt, organisatorisk eller teknisk tiltak som etableres for å hindre at en sikkerhetshendelse inntreffer. |
| Tilgjengelighet | Å sikre autoriserte brukeres tilgang til informasjon og tilhørende ressurser ved behov. |

# sikkerhetsMÅL

Sikkerhetsmålene skal understøtte og sikre avdelingens drift, allmenn tillitt og omdømme ved å forebygge og begrense konsekvensene av uønskede hendelser.

Sikkerhetsmålene beskriver avdelingens overordnede mål for beskyttelse av avdelingens informasjonsbehandling mot interne og eksterne trusler av tilsiktet og utilsiktet art.

Følgende sikkerhetsmål er definert:

* Avdelingen skal sikre at informasjon behandles iht. krav i relevante lover og forskrifter.
* Den fysiske sikkerheten i avdelingen skal hindre at uautoriserte får tilgang til lokaler der beskyttelsesverdig informasjon og sensitive personopplysninger lagres og behandles.
* Tilgang til systemer og informasjon gis kun til medarbeidere etter behov.
* Avdelingen skal sikre tilgjengelighet til systemer, tjenester og informasjon til rett tid for de personer som er autorisert.
* Avdelingen skal sikre at kvaliteten på informasjonen er gyldig, nøyaktig og fullstendig.
* Avdelingen skal sikre at medarbeidere som bruker avdelingens informasjonssystemer har tilstrekkelig kompetanse for å ivareta virksomhetens sikkerhetsbehov/krav.
* Enhver som henvender seg til forbundet og ber om det, vil bli opplyst om hvilke typer personopplysninger som blir behandlet i avdelingen. Dersom det viser seg at behandlingene omfatter opplysninger om vedkommende, vil det bli gitt innsyn i disse.
* Avdelingen skal kun benytte databehandlere som forplikter seg gjennom avtaler om å behandle forbundets personopplysninger i samsvar med kravene i personopplysningsloven.

# Roller og ansvar FOR informasjonssikkerhet

## Avdelingsleder

Avdelingsleder er overordnet ansvarlig for informasjonssikkerheten. Avdelingsleder er formelt behandlingsansvarlig, men kan delegere dette til andre i avdelingen der det er hensiktsmessig.

Det skal også utpekes en sikkerhetsansvarlig i avdelingen. Hvis det er hensiktsmessig, kan avdelingsleder ivareta denne rollen.

Avdelingsleder har ansvar for å gjøre regelverket for informasjonssikkerhet kjent i avdelingen.

## Behandlingsansvarlig

Behandlingsansvarlig er den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes. Rollen er lovbestemt.

Behandlingsansvarlig har ansvar for:

* at behandlingen av personopplysninger foregår i tråd med lovens bestemmelser
* at det foreligger oppdaterte databehandleravtaler med leverandører som behandler avdelingens data
* at medarbeidere som behandler personopplysninger benytter informasjonssystemet i samsvar med avdelingens rutiner
* å gjennomføre risikovurderinger ved ny behandling av personopplysninger

## Sikkerhetsansvarlig

Sikkerhetsansvarlig har ansvaret for:

* at «Styringssystemet for informasjonssikkerhet» er i tråd med lovkrav og tilpasset avdelingen
* å iverksette sikkerhetstiltak som er nødvendig for å sikre stabil drift og tilstrekkelig sikkerhet
* å behandle sikkerhetsavvik
* å tilrettelegge sikkerhetsopplæring for nye medarbeidere

## øvrige ansatte og tillitsvalgte

Ansatte/tillitsvalgte plikter å behandle informasjon i samsvar med regelverket for informasjonssikkerheten og har ansvar for å melde fra om sikkerhetsavvik.

# 

# OVERSIKT OVER BEHANDLING AV PERSONOPPLYSNINGER

| **Formålskategori** | **System** | **Hvilke typer persondata behandles?** | **Behandles sensitive data, i så tilfelle hvilke?** | **Behandlings­ansvarlig** | **Databehandlere** |
| --- | --- | --- | --- | --- | --- |
| **Administrasjon av medlemmer** | ACOS WebSak  Pluss | **Sivilrettslige- og kollektive saker**  - Personopplysninger  - Tvisteforhold  - Helseopplysninger  - Fagforeningsmedlemskap | Helse- og  strafferettslige forhold | Avdelingsleder | Fellesforbundet |
| Fane2 | **Fagforeningsmedlemskap**  Medlemsopplysninger | Fagforeningsopplysning | Fellesforbundet  sentralt | Advania |
| **Administrasjon av tillitsvalgte** | Fane2 | **Tillitsvalgte**  Tillitsvalgtopplysninger | Fagforeningsopplysning | Fellesforbundet  sentralt | Advania |
|  |  |  |  |  |
| **Administrasjon av personal-opplysninger** | Lønn- og regnskapssystem | **Personaladministrasjon**  - Lønn/fravær/trekk | Fagforeningstilhørighet | Avdelingsleder | Firma X |
|  |  |  |  |  |
| Andre systemer? |  |  |  |  |
|  |  |  |  |  |

Jfr. forslag til mal for

* "Kartleggingsskjema – Systemer"
* "Systemoversikt – Ansatte og valgte i avdelingen"
* "Systemoversikt – Medlemmer i avdelingen"

# 6. RUTINER

## 6.1 Avdelingsstyrets gjennomgang

Sikkerhetsansvarlig har ansvaret for å vedlikeholde «Styringssystemet for informasjonssikkerhet». Systemet gjennomgås av avdelingsstyret minst en gang per år eller ved behov dersom det skjer endringer i perioden.

## 6.2 risikovurdering

Sikkerhetsansvarlig er ansvarlig for at det gjennomføres risikovurderinger ved ny behandling av personopplysninger eller ved endringer som kan påvirke informasjonssikkerheten.  
  
Ved risikovurderingen skal en

* vurdere nye risikoforhold (trusler) som følge av endringer. Endringer kan skyldes endring i trusselbildet, konfigurasjon, arbeidsrutiner, organisasjon, nye systemer osv.
* vurdere sannsynlighet for at sikkerhets­hendelser inntreffer som følge av endringer i risikoforhold
* vurdere om risiko er på et akseptabelt nivå
* iverksette tiltak som kan redusere risiko til akseptabelt nivå

## 6.3 Retten til innsyn, retting og sletting

De som avdelingen håndterer personopplysninger om, har rett til å få innsyn i personopplysningene. De har rett til å få rettet opplysningene hvis de er feil og de har rett til å få slettet opplysningene hvis man ikke har et lovlig formål i forhold til hva som er registrert.

Når det gjelder krav om innsyn i Fane2, skal medlemmene rette henvendelsen til forbundet v/ behandlingsansvarlig.

Hvis et medlem/ansatt ber om innsyn i det som er registrert i ACOS WebSak Pluss og avdelingen har avtale om bruk av den lokale saksbehandlingsløsningen, vil forbundet v/behandlingsansvarlig og arkiv være avdelingen behjelpelig med å håndtere dette.

En innsynsbegjæring kan avlede et ønske om "retten til å bli glemt". Det er viktig å skille mellom informasjon avdelingen har lagret om individer for å opplyse forpliktelser eller som er lovbestemt, opp mot det som er lagret over tid som ikke har relevans for avdelingenes forpliktelser. Dette kan være påloggingsinformasjon, søkeinformasjon, logging, privat e-post o.l.

Jfr. forslag til mal for

* "Rutine - Innsyn, retting og sletting – Ansatte og valgte i avdelingen"
* "Rutine – Innsyn, retting og sletting – Medlemmer i avdelingen"
* "Skjema for krav om innsyn, retting og sletting – Ansatte og valgte i avdelingen"
* "Skjema for krav innsyn, retting og sletting – medlemmer i avdelingen"

## 6.4 Personvernerklæring

Alle skal ha en oppdatert og forståelig personvernerklæring.

Jfr. forslag til mal for

* "Personvernerklæring – Ansatte og valgte i avdelingen"
* "Personvernerklæring – Medlemmer i avdelingen"

## 6.5 Inngåelse av databehandleravtaler

En databehandleravtale skal sikre at personopplysninger blir behandlet i samsvar med regelverket og setter en klar ramme for hvordan databehandleren kan behandle opplysninger.

Når det gjelder databehandleravtale i tilknytning til Fane2, så har forbundet en overordnet databehandleravtale med leverandøren Advania i egenskap av å være behandlingsansvarlig. Det er kun behandlingsansvarlig som kan inngå databehandleravtaler.

Jfr. forslag til mal for

* «Databehandleravtale»

## 6.6 Avviksbehandling

Dersom informasjonssystemet benyttes i strid med fastlagte rutiner, ved brudd på informasjonssikkerheten samt mistanke om sikkerhetsbrudd, iverksettes avviksbehandling, jf. rutine for avviksrapportering.

Avvik kan imidlertid ikke unngås helt, og selve avviket vil inneholde informasjon som er viktig i en prosess der kontinuerlige sikkerhetsforbedringer er målet. Det er derfor nødvendig med systematisk behandling av avvik, både for å begrense skade og hindre gjentagelse.

## 6.7 Overføring av personopplysninger

Generelt skal ekstern overføring av personopplysninger beskyttes. Overføring av personopplysninger uten beskyttelse kan kun gjennomføres dersom den registrerte selv samtykker til en slik overføring. Fødselsnummer skal kun brukes ved behov og sikres med kryptering ved elektroniske forsendelser.

## 6.8 Opplæring (Sikkerhet)

Når ansatte/tillitsvalgte i avdelingen og eventuelle tredjepartsbrukere får tilgang til informasjon eller tjenester, skal disse ha en hensiktsmessig opplæring slik at de har forutsetninger for å følge rutiner og pålagte sikkerhetstiltak

# 7. Vedlegg

Følgende forslag til maler finner dere i dokumentet «Vedlegg – Styringssystem for informasjonssikkerhet»:

Mal 2 – Kartleggingsskjema for avdelingene – Systemer

Mal 3 – Systemoversikt – Ansatte og valgte i avdelingen

Mal 4 – Systemoversikt – Medlemmer i avdelingen

Mal 5 – Rutine – Innsyn, retting og sletting – Ansatte og valgte i avdelingen

Mal 6 – Rutine – Innsyn, retting og sletting – Medlemmer i avdelingen

Mal 7 – Skjema for krav om innsyn, retting og sletting – Ansatte og valgte i avdelingen

Mal 8 – Skjema for krav om innsyn, retting og sletting – Medlemmer i avdelingen

Mal 9 – Personvernerklæring – Ansatte og valgte i avdelingen

Mal 10 – Personvernerklæring – Medlemmer i avdelingen

Mal 11 – Databehandleravtale

Mal 12 – Avviksrapportering

1. Ved vurdering av sikkerhetsbehovet knyttet til opplysninger om fagforeningsmedlemskap, kan det nevnes at konfidensialitet sikring normalt vil være mindre nødvendig ved behandling av opplysninger om fagforeningstilhørighet enn for behandling av sensitive personopplysninger for øvrig. [↑](#footnote-ref-1)