**Vedlegg**

**Styringssystemet for informasjonssikkerhet (Mal 1)**

**Innhold**

[Kartleggingsskjema 2](#_Toc101959998)

[Systemoversikt – Ansatte og valgte i avdeling x 3](#_Toc101959999)

[Systemoversikt – Medlemmer i avdeling x 4](#_Toc101960000)

[Rutine for innsyn, retting og sletting ansatte og valgte 8](#_Toc101960001)

[Rutine for innsyn, retting og sletting medlemmer 9](#_Toc101960002)

[Innsynsskjema - Personalinformasjon 10](#_Toc101960003)

[innsynsskjema - Medlemsinformasjon 12](#_Toc101960004)

[Personvernerklæring for ansatte og valgte i avdeling x 14](#_Toc101960005)

[Personvernerklæring for medlemmer i avdeling x 19](#_Toc101960006)

[Databehandleravtale 22](#_Toc101960007)

[Avviksrapportering 28](#_Toc101960008)

*Forslag til MAL 2*

# Kartleggingsskjema

**System:** Klikk her for å skrive inn tekst.

**Avdeling:** **Behandlingsansvarlig:** Klikk her for å skrive inn tekst.

*(Den som bestemmer formålet med behandlingen av personopplysninger)*

**Vurdert av:** Klikk her for å skrive inn tekst. **Dato:** Klikk her for å skrive inn en dato.

1. **Behandles persondata i systemet/rutinen? JA  NEI**

*(Personopplysninger som kan knyttes til en enkelt person, f.eks. navn, adresse, telefonnummer, e-post og fødselsnummer).*

1. **Hvis JA, hvilke persondata behandles og hva er formålet:**
2. **Er det registrert sensitive data om enkeltpersoner? JA  NEI***(Opplysninger om rasemessig eller etnisk bakgrunn, politisk, filosofisk eller religiøs oppfatning, siktet, tiltalt eller dømt. I tillegg kommer helseforhold, seksuelle forhold eller medlemskap i fagforeninger).*
3. **Hvis JA, hvilke sensitive data behandles og hva er formålet?**
4. **Brukes det databehandler til å håndtere dataene som systemet/rutinen benytter?***(En juridisk enhet som behandler personopplysninger på vegne av den behandlingsansvarlige).* **JA  NEI**
5. **Utveksles data med eksterne og i så tilfelle hvordan?**
6. **Kommentarer eller annen informasjon:**

*Forslag til MAL 3*

# Systemoversikt – Ansatte og valgte i avdeling x

Systemer **hvor avdeling x er behandlingsansvarlig**[[1]](#footnote-1) og hvor innsyn, retting eller sletting skal rettes til avdeling x.

*NB!*

*Eksempel på utfylling. Dette må tilpasses i forhold til de systemene avdelingen har.*

|  |  |
| --- | --- |
| **Papirbaserte personalmapper** | |
| * Hvilke opplysninger er registrert? | *Personal- og identifikasjonsopplysninger herunder. helseopplysninger i forbindelse med sykefraværsoppfølging og yrkesskade samt disiplinærsak.* |
| * Hva er formålet? | *Oppbevare relevante opplysninger om ansettelsesforholdet.* |
| * Hva er behandlingsgrunnlaget? | *Artikkel 6 i personvernforordningen* |
| * Hvordan håndteres retting/sletting? | *Her må det beskrives hvor lenge dere oppbevarer personalmappene til de som avslutter sitt arbeidsforhold, går av med pensjon mv. Hvor lenge oppbevares opplysningene som ligger i personalmappene, hvordan håndteres retting og sletting osv.*  *Husk at det skal være et formål med alt som oppbevares.*  *Retting utføres fortløpende.* |

|  |  |
| --- | --- |
| **Elektronisk personalarkiv** – avdeling x | |
| * Hvilke opplysninger er registrert? | *Personal- og identifikasjonsopplysninger herunder helseopplysninger i forbindelse med sykefraværsoppfølging og yrkesskade samt disiplinærsaker.* |
| * Hva er formålet? | *Å ha et system for personaladministrasjon, samt identifikasjonsopplysninger knyttet til nåværende og tidligere ansatte.*  *Oppbevare relevante opplysninger om ansettelsesforholdet.* |
| * Hva er behandlingsgrunnlaget? | *Artikkel 6 i personvernforordningen* |
| * Hvordan håndteres retting/sletting? | *Her må det beskrives hvor lenge dere oppbevarer personalmappene til de som avslutter sitt arbeidsforhold, går av med pensjon mv. Hvor lenge oppbevares opplysningene som ligger i personalmappene, hvordan håndteres retting og sletting osv.*  *Husk at det skal være et formål med alt som oppbevares.*  *Retting utføres fortløpende.* |
| * Hvordan håndteres innsyn? | *Innsyn håndteres iht. rutinen "Innsyn, retting og sletting". Se vedlegg.*  *Avdeling x kan kontakte fellestjenester for bistand til innsynet dersom de har ACOS WebSak Fokus.* |
| * Utleveres opplysninger fra systemet? | *Opplysninger av historisk interesse og verdi avleveres til arkivdepot..* |

|  |  |
| --- | --- |
| **Adgangskort** | |
| * Hvilke opplysninger er registrert? | *Hvis dere har et system for dette.*  *Navn, kode, kortnummer, tilganger i avdelingens lokaler, bilde av den ansatte.* |
| * Hva er formålet? | *Opprettelse av adgangs-/nøkkelkort slik at den ansatte kommer inn i de lokalene vedkommende skal ha tilgang til.* |
| * Hva er behandlingsgrunnlaget? | *Artikkel 6 i personvernforordningen* |
| * Hvordan håndteres retting/sletting? | *Må beskrives* |
| * Hvordan håndteres innsyn? | *Innsyn håndteres iht. rutinen "Innsyn, retting og sletting". Se vedlegg.* |
| * Utleveres opplysninger? | *Det utleveres ikke opplysninger til 3. part.* |

|  |  |
| --- | --- |
| **Avdelingens hjemmeside** | |
| * Hvilke opplysninger er registrert? | *Navn, tittel, telefonnummer, e-postadresse, bilde.* |
| * Hva er formålet? | Yte service. |
| * Hva er behandlingsgrunnlaget? | Artikkel 6 i personvernforordningen,  Samtykke til ansattbilde |
| * Hvordan håndteres retting/sletting? | *Må beskrives* |
| * Hvordan håndteres innsyn? | *Den ansatte/valgte kan selv se hvilke opplysninger som ligger på forbundets hjemmeside.* |
| * Utleveres opplysninger? | Det utleveres ikke opplysninger til 3. part. |
| * Annet |  |

|  |  |
| --- | --- |
| **Lønns- og regnskapssystem (dersom avdelingen har dette)** | |
| * Hvilke opplysninger er registrert? | *Navn, fødselsnummer, adresse, skatteopplysninger,*  *e-postadresse, mobilnummer, fagforeningstilhørighet, ansattdato og lønnshistorikk.* |
| * Hva er formålet? | *Myndighetene stiller krav til hvilke personopplysninger det skal rapporteres på i forbindelse med den månedlige lønnsinnberetningen i Altinn.* |
| * Hva er behandlingsgrunnlaget? | *Gjeldende skatteregler, bokføringslov og regnskapslov* |
| * Hvordan håndteres retting/sletting? | *Data oppbevares i 5 år iht. gjeldende skatteregler samt anbefaling fra revisor.* |
| * Hvordan håndteres innsyn? | *Innsyn håndteres iht. rutine "Innsyn, retting og sletting".* |
| * Utleveres opplysninger? | *Det utleveres ingen opplysninger til 3. part annet enn månedlig innrapportering til Altinn.* |
| * Annet | *Det er inngått databehandleravtale med leverandør X.* |

**ANNET**

|  |
| --- |
| **Fane2 medlemshåndteringssystem** |
| Noen ansatte er også medlemmer i Fellesforbundet og dermed registrert i Fane2 medlemshåndteringssystem. Når det gjelder håndtering av dette, henvises det til systemoversikten som gjelder medlemmer. |

|  |
| --- |
| **Åpning av post med mottakers navn først** |
| *Åpning av post hvor mottakers navn står øverst, krever samtykke.* |

|  |
| --- |
| **Arbeiderbevegelsens Arkiv og bibliotek (Arbark)** |
| *Opplysninger som er av historisk interesse avleveres.* |

|  |
| --- |
| **Multimaskiner** |
| Det blir sendt over et bilde av dokumentet til den maskinen som dokumentet skrives ut på. Bildet/fila av det som blir skrevet ut, kopiert og skannet inn blir liggende i minnet på multimaskinen.  På multimaskinens minne logges det hvem som har skrevet ut dokumenter og når dokumentene ble skrevet ut.  Det er mulig å sladde dokumentet, dvs. at det kun er tittelen på fila som vises.  Minnet på maskiner som leveres tilbake for kondemnering eller gjenbruk, blir slettet. |



*Forslag til MAL 4*

# Systemoversikt – Medlemmer i avdeling x

Systemer **hvor avdelingen er behandlingsansvarlig[[2]](#footnote-2)** og hvor innsyn, retting eller sletting skal rettes til avdelingen:

*NB!*

*Eksempel på utfylling. Dette må tilpasses i forhold til de systemene avdelingen har.*

|  |  |
| --- | --- |
| **ACOS WebSak Pluss saksbehandlingssystem** – Gjelder de avdelinger som har databehandleravtale med forbundet om bruk av lokal saksbehandlingsløsning | |
| * Hvilke opplysninger er registrert? | *Persondata inkludert fødselsnummer samt andre opplysninger som har relevans for saken.*  *Sivilrettslige og kollektive saker, f.eks. lønnskrav, yrkesskader og oppsigelser.* |
| * Hva er formålet? | *Formålet er å bistå medlemmer i sivilrettslige saker og ha et sikkert system for juridisk dokumentasjon.* |
| * Hva er behandlingsgrunnlaget? | *Artikkel 6 i personvernforordningen* |
| * Hvordan håndteres retting/sletting? | *Retting foretas fortløpende.*  *Fellesforbundet v/arkivet bistår avdelingen ved retting og sletting.* |
| * Hvordan håndteres innsyn? | *Innsyn håndteres iht. rutinen "Innsyn, retting og sletting". Se vedlegg.*  *Fellesforbundet v/arkivet bistår avdelingen ved innsyn.* |
| * Annet | *Det er inngått databehandleravtale med Fellesforbundet.* |

|  |  |
| --- | --- |
| **Lønns- og regnskapssystem** (dersom avdelingen har dette) | |
| * Hvilke opplysninger er registrert? | *Navn, fødselsnummer, adresse, skatteopplysninger,*  *e-postadresse, mobilnummer, fagforeningstilhørighet, ansattdato og lønnshistorikk.* |
| * Hva er formålet? | *Myndighetene stiller krav til hvilke personopplysninger det skal rapporteres på i forbindelse med den månedlige lønnsinnberetningen i Altinn.* |
| * Hva er behandlingsgrunnlaget? | *Gjeldende skatteregler, bokføringslov og regnskapslov.* |
| * Hvordan håndteres retting/sletting? | *Data oppbevares i 5 år iht. gjeldene skatteregler samt anbefaling fra revisor.* |
| * Hvordan håndteres innsyn? | *Innsyn håndteres iht. rutine, "Innsyn, retting og sletting".* |
| * Utleveres opplysninger fra systemet? | *Det utleveres ingen opplysninger til 3. part annet enn månedlig rapportering til Altinn.* |
| * Annet | *Det er inngått databehandleravtale med leverandør x.* |

**Andre systemer, eks. saksbehandlingssystem, kurssystem e.l.**

Systemer **hvor andre enn avdelingen er behandlingsansvarlig** og hvor innsyn, retting eller sletting kan rettes direkte til behandlingsansvarlig:

|  |  |
| --- | --- |
| **FANE2 medlemshåndteringssystem** –  Avdeling for drift, sikkerhet og digitale tjenester er behandlingsansvarlig | |
| * Hvilke opplysninger er registrert? | Navn, adresse, fødselsnummer, kontaktinformasjon, arbeidsgiverinformasjon, kontingentopplysninger, innmeldingsdato, avdelingstilhørighet og tillitsverv i Fellesforbundets regi. |
| * Hva er formålet? | Administrasjon av medlemmer i samsvar med forbundets formål gjengitt i vedtektene. |
| * Hva er behandlingsgrunnlaget? | Artikkel 6 i personvernforordningen  Oppbevaringsplikt iht. skatteopplysninger ved innbetaling av kontingent til Altinn og historiske data iht. vedtekter. |
| * Hvordan håndteres retting/sletting? | **NB! Ordinært vedlikehold foretas fortløpende på vanlig måte.**  Retting og sletting iht. innsynsbegjæringer rettes til forbundet v/medlems- og økonomiavdelingen. |
| * Hvordan håndteres innsyn? | Innsyn rettes til forbundet v/medlems- og økonomiavdelingen. |
| * Utleveres opplysninger? | Det overføres opplysninger til LOfavør AS, Veiviseren, LO Media (Magasinet for fagorganiserte), Strålfors, Nets (betalingsmottak til bankene), Altinn og Fellesforbundets medlemsportal. I forbindelse med medlemsundersøkelser overføres det også kontaktinformasjon til Opinion og Ipsos.  E-postadresser tas ut for utsendelse av nyhetsbrev til medlemmer.  Telefonnummer tas ut for utsendelse av SMS til medlemmer.  Opplysninger tas også ut for gjennomføring av medlemsundersøkelser. |

**ANNET:**

|  |
| --- |
| **Facebook** – Gjelder avdelinger som har egen FaceBook-profil |
| *Avdelingens Facebook-side brukes først og fremst for å nå fram til eksisterende og potensielle medlemmer med saker om vårt arbeid og den politikken vi jobber for å få gjennomslag for. Ved hjelp av Facebook sitt eget markedsførings- og analyseverktøy målretter vi av og til innhold til de spesifikke gruppene i befolkningen vi ønsker å nå, det være seg demografisk tilhørighet eller yrkesgrupper/interesser. Dette er viktig for oss fordi vi organiserer innenfor vidt forskjellige bransjer, og ønsker dermed å kunne tilby relevant informasjon til de ulike medlemsgruppene våre. Det er imidlertid ikke snakk om direkte kommersiell virksomhet, utover det å oppfordre til å bli medlem hos oss.* |

|  |
| --- |
| **Ulike sosiale medier** – Gjelder avdelinger som benytter andre sosiale medier |
| *Ved registrering til arrangementer eller lignende kan det være hensiktsmessig å beskrive at ved å bruke denne tjenesten samtykker du til at avdelingen benytter den informasjonen du selv velger å oppgi til å gi deg relevant informasjon om eksempelvis arrangementet. Vi lagrer ikke informasjon om deg etter at arrangementet er gjennomført og vi gir det ikke videre til tredjepart.* |

|  |
| --- |
| **Arkivdepot** |
| *Opplysninger som er av historisk interesse avleveres til arkivdepot.* |

|  |
| --- |
| **Generelt** |
| Det pågår et samarbeid mellom flere forbund i tilknytning til medlemshåndtering hvor man blant annet ser på oppbevaring av medlemshistorikk, behov for samtykke og reservasjonsmuligheter. |

**Det er viktig å gjøre oppmerksom på at det også finnes personinformasjon i Fellesforbundet.**



*Forslag til MAL 5*

# Rutine for innsyn, retting og sletting ansatte og valgte

**Kategori:** Ansatte, valgte, tidligere ansatte og tidligere valgte

**Formål:** Administrasjon av personalopplysninger

**Ansvarlig:** *Avdeling x / person x*

**Frist for tilbakemelding:** Uten ugrunnet opphold, normalt senest innen en måned

**Innsyn:**

* Den som ønsker innsyn må fylle ut skjemaet *"Krav om innsyn, retting eller sletting"*
* Person x bekrefter på samme skjema at det er riktig person
* Saken registreres og skjemaet arkiveres.
* Person x innhenter opplysninger fra de relevante systemene innen en frist. *Jf "Systemoversikt – ansatte og valgte i avdelingen"*
* Person x gir tilbakemelding til den som ønsker innsyn og sørger for nødvendig dialog fram til saken kan avsluttes.
* Saksbehandlingen dokumenteres.

**Retting:**

* Den som ønsker retting må fylle ut skjemaet *"Krav om innsyn, retting eller sletting"*
* Person x bekrefter på samme skjema at det er riktig person.
* Saken registreres og skjemaet arkiveres.
* Person x må innen en frist få tilbakemelding på at opplysningene er rettet*. Jf "Systemoversikt – ansatte og valgte i avdelingen "*
* Person x gir samlet tilbakemelding til den som ønsker retting og bekrefter at retting er utført i alle relevante systemer.
* Saksbehandlingen dokumenteres.

**Sletting:**

* Den som ønsker sletting må fylle ut skjemaet *"Krav om innsyn, retting eller sletting"*
* Person x bekrefter på samme skjema at det er riktig person.
* Saken registreres og skjemaet arkiveres.
* Person x må innen en frist få tilbakemelding på at opplysningene er slettet og dokumentasjon på dette eller hvordan saken kan håndteres og dokumenteres. *Jf "Systemoversikt – ansatte og valgte i avdelingen"*
* Person x gir samlet tilbakemelding til den som ønsker sletting om hva som er utført.
* Saksbehandlingen dokumenteres.



*Forslag til MAL 6*

# Rutine for innsyn, retting og sletting medlemmer

**Kategori:** Medlemmer og tidligere medlemmer

**Formål:** Administrasjon av medlemsopplysninger

**Ansvarlig:** Avdeling x

**Frist for tilbakemelding:** Uten ugrunnet opphold, normalt senest innen en måned

**Innsyn:**

* Den som ønsker innsyn må fylle ut skjemaet *"Krav om innsyn, retting eller sletting"*
* Avdeling x bekrefter på samme skjema at det er riktig person[[3]](#footnote-3)
* Saken registreres og skjemaet arkiveres.
* Avdeling x innhenter relevante opplysninger, *jf. "Systemoversikt – medlemmer i avdelingen".*
* Avdeling x gir tilbakemelding til den som ønsker innsyn og forestår nødvendig dialog fram til saken kan avsluttes.
* Saksbehandlingen dokumenteres.

**Retting:**

* Den som ønsker retting må fylle ut skjemaet *"Krav om innsyn, retting eller sletting"*
* Avdeling x bekrefter på samme skjema at det er riktig person
* Saken registreres og skjemaet arkiveres.
* Avdeling x innhenter relevante opplysninger, *jf. "Systemoversikt – medlemmer i avdelingen".*
* Avdeling x gir tilbakemelding til den som ønsker retting og forestår nødvendig dialog fram til saken kan avsluttes.
* Saksbehandlingen dokumenteres.

**Sletting:**

* Den som ønsker retting må fylle ut skjemaet *"Krav om innsyn, retting eller sletting"*
* Avdeling x bekrefter på samme skjema at det er riktig person
* Saken registreres og skjemaet arkiveres.
* Avdeling x innhenter relevante opplysninger, *jf. "Systemoversikt – medlemmer i avdelingen".*
* Avdeling x gir tilbakemelding til den som ønsker sletting og sørger for nødvendig dialog fram til saken kan avsluttes.
* Saksbehandlingen dokumenteres.



*Forslag til MAL 7*

# Innsynsskjema - Personalinformasjon

**Skjema for krav om innsyn, retting eller sletting**

**Navn (**blokkbokstaver**): ……………………………………………………………**

**Adresse: …………………………………………………………………………….**

**Postnr/sted: …………………………………………………………………………**

**Fødselsdato: ………………………………………….**

**Underskrift: …………………………………………………………………………**

**Avdeling x bekrefter at ovennevnte informasjon er korrekt:**

**Dato: …………………… Underskrift: ………………………………………….**

|  |
| --- |
| **Ønskes det innsyn?** |
| Hva ønskes det innsyn i? |

|  |
| --- |
| **Ønskes det retting?** |
| Hva ønskes rettet? |

|  |
| --- |
| **Ønskes det sletting?** |
| Hva ønskes slettet? |



*Forslag til MAL 8*

# innsynsskjema - Medlemsinformasjon

**Skjema for krav om innsyn, retting eller sletting**

**Navn (**blokkbokstaver**): ……………………………………………………………**

**Adresse: …………………………………………………………………………….**

**Postnr/sted: …………………………………………………………………………**

**Fødselsdato: ………………………………………….**

**Avdeling: ……………………………………………………………………………**

**Underskrift: …………………………………………………………………………**

**Avdeling x bekrefter at ovennevnte informasjon stemmer:**

**Dato: …………………… Underskrift: ………………………………………….**

|  |
| --- |
| **Ønskes det innsyn?** |
| Hva ønskes det innsyn i? |

|  |
| --- |
| **Ønskes det retting?** |
| Hva ønskes rettet? |

|  |
| --- |
| **Ønskes det sletting?** |
| Hva ønskes slettet? |



*Forslag til MAL 9*

# Personvernerklæring for ansatte og valgte i avdeling x

(Organisasjonsnummer x)

**Sist oppdatert 26.04.2022**

[](https://www.google.com/url?sa=i&rct=j&q=&esrc=s&source=images&cd=&cad=rja&uact=8&ved=2ahUKEwiu1-Hzm_HbAhXlNJoKHfFTBsEQjRx6BAgBEAU&url=https://www.civita.no/politisk-ordbok/hva-er-rettsliggjoring/paragraf&psig=AOvVaw2R5S_QLJAmokQfiJ1qYA-M&ust=1530098628810046)

1. **Innledning**

Avdelingsleder er behandlingsansvarlig[[4]](#footnote-4) for de personopplysninger vi har registrert og behandler i forbindelse med ditt ansettelsesforhold/verv i *avdeling x*.  
  
Denne personvernerklæringen gir deg informasjon om hvordan vi behandler dine personopplysninger og hvilke rettigheter du har.

1. **Personopplysninger som *avdeling x* registrerer**

Personopplysninger er alle opplysninger som kan knyttes til deg som enkeltperson.

**2.1 Opplysninger vi registrerer om deg som ansatt/valgt**

*Eksempel på utfylling. Dette må tilpasses i forhold til hva avdelingen gjør.*

*Vi registrerer ditt navn, adresse, fødselsnummer, e-postadresse og telefonnummer. I tillegg oppbevarer vi kontonummer for utbetaling av lønn. For å registrere antall sykedager i forbindelse med sykt barn, trenger vi opplysninger om antall barn og alder.  
  
I forbindelse med ansettelsesprosessen lagrer vi din CV for resten av ansettelsesforholdet og uttalelser fra referanser og interne vurderinger inntil utløpt prøvetid.  
  
Det er nødvendig å behandle dine helseopplysninger i forbindelse med sykefravær og sykemeldinger samt tilhørende sykefraværsoppfølging. HMS-regelverket gjør det nødvendig å lagre opplysninger om personskader og ulykker.  
  
Fagforeningsmedlemskap lagres dersom dette er nødvendig for trekk av kontingent eller avlønning.*

**2.2 Opplysninger vi registrerer i forbindelse med ditt arbeidsforhold**

*Eksempel på utfylling. Dette må tilpasses i forhold til hva avdelingen gjør.*

*Det vil være opplysninger som ansettelsesdato, stilling, stillingsbeskrivelse, lønnsutvikling og informasjon knyttet til din kompetanseutvikling og ditt arbeidsforhold. Kildene for slik informasjon vil i hovedsak komme fra våre informasjonssystemer, jf. "Systemoversikt – ansatte og valgte i avdeling x".*

*Vi lagrer informasjon om utlegg, andre utgifter, forsikringer, pensjon, kredittkort som avdelingen svarer for etc.  
  
Vi registrerer personopplysninger i forbindelse med permisjoner, pensjon og avslutning av ansettelsesforholdet.  
  
Håndtering av advarsler, varsling og klager kan nødvendiggjøre behandling av dine personopplysninger, enten du er varsler eller om noen skulle varsle om deg.   
  
Bruk av våre informasjonssystemer vil genere ulike typer aktivitetslogger. Disse kan f.eks. gi informasjon om når du bruker et datasystem og når du benytter adgangskontrollsystemet.*

**2.3 Hva avdeling X bruker personopplysningene til**

Det rettslige grunnlaget for behandling av personopplysninger er enten at behandlingen er nødvendig for å oppfylle arbeidsavtalen vi har med deg, at vi er pålagt behandlingen i lov eller at vi har en berettiget interesse i behandlingen som overskrider eventuell personvernmessig ulempe for deg.

Under angis de mest sentrale formålene personopplysningene brukes til:

*Eksempel på utfylling. Dette må tilpasses i forhold til hva avdelingen gjør.*

* *Vi trenger å administrere arbeidsforholdet og din kompetanseutvikling og bruker de mange ulike opplysningene som generes mens du er ansatt til dette.*
* *Vi trenger å utbetale lønn og andre økonomiske kompensasjoner, samt pensjonsforpliktelser og forsikringsordninger og bruker dine lønnsrelaterte opplysninger til dette.*
* *Vi trenger å sikre våre systemer og avdelingens lokaler samt å trygge sikkerhet på arbeidsplassen og benytter informasjon fra ulike systemer og logger fra adgangs-kontrollsystemer for dette.*
* *Vi trenger å behandle klager, varsler og advarsler og bruker de mange ulike opplysningene som genereres mens du er ansatt i avdelingen.*
* *Vi trenger å registrere opplysninger for bokføringsformål og bruker dine lønnsrelaterte opplysninger til dette.*
* *Vi kan ønske å bruke ditt bilde på vår hjemmeside for å yte bedre service, men dette gjøres kun på basis av ditt samtykke og du står fritt til å trekke ditt samtykke tilbake.*

1. **Hvem deler vi dine opplysninger med**

Vi benytter databehandlere[[5]](#footnote-5) som bistår oss med ulike prosesser i *avdeling x*. Ulike typer kategorier av databehandlere er angitt under:

*Eksempel på utfylling. Dette må tilpasses i forhold til hva avdelingen gjør.*

* *Leverandører som drifter IT- og telefonisystemer*
* *Leverandør som bistår oss med lønn og reiseregninger*
* *Leverandører som bistår med sikkerhet, f.eks. adgangskontrollsystemer*

*Offentlige myndigheter pålegger oss å dele dine personopplysninger med skatteetaten og NAV.*

*Avdeling x har inngått en IT-driftsavtale med leverandør X. Leverandør X har ansvar for sikring av avdelingens systemer i overenstemmelse med GDPR[[6]](#footnote-6).*

*Se for øvrig "Systemoversikt – Ansatte og valgte i avdeling x".*

1. **Geografisk lagring av personopplysninger**

*Eksempel på utfylling. Dette må tilpasses i forhold til hvordan avdelingen håndterer dette.*

*I utgangspunktet lagres ikke personopplysninger utenfor Norge, men noen driftsleverandører har driftssenter i EU/EØS hvor GDPR følges.*

1. **Hvor lenge lagrer vi opplysningene om deg**

*Eksempel på utfylling. Dette må tilpasses i forhold til hvordan avdelingen håndterer dette.*

*Avdeling x lagrer dine personopplysninger så lenge det er nødvendig, eller vi er pålagt lagring etter lov. Vi har behov for* ***flere*** *opplysninger om deg mens du er ansatt og* ***færre*** *etter at arbeidsforholdet er avsluttet.*

*Vi vil uansett lagre opplysninger så lenge det følger av lov, og der hvor det oppstår et særlig behov, f.eks. ved klager eller krav som rettes mot oss eller av oss.*

1. **Dine rettigheter**

Personvernregelverket gir deg rettigheter knyttet til dine personopplysninger:

* Selv om denne personvernerklæringen gir mye informasjon, kan du be om mer inngående informasjon om hvordan vi behandler opplysninger om deg og du har rett til innsyn i dine personopplysninger. Dersom dine personopplysninger er feil, har du rett til å få dem rettet. Personopplysninger som vi eventuelt ikke har grunnlag for å behandle, skal slettes og du kan kreve dette gjort om vi ikke har sørget for dette på eget initiativ. Du kan også be om at vi begrenser bruk av dine opplysninger.
* Hvis du mener at vi behandler dine opplysninger uten rettslig grunnlag, kan du klage til Datatilsynet, men vi anmoder deg om å kontakte *avdeling x* slik at vi kan ta stilling til dine innvendinger og at vi kan oppklare eventuelle misforståelser.
* Dersom du ønsker å gjøre bruk av dine rettigheter henvender du deg til *avdeling x/person x* og din henvendelse vil, etter at personvernforordningen har trådt i kraft i Norge, bli besvart innen 30 dager. Se "Rutine – innsyn, retting og sletting" samt "Skjema for krav om innsyn, retting eller sletting".

1. **Innsyn i e-post**

*Dersom avdelingen praktiserer dette, bør teksten under stå i erklæringen.*

Personvernregelverket åpner for at avdelingen i bestemte tilfeller kan foreta innsyn i din

e-postkasse og annet utstyr som er stillet til rådighet for deg. Typisk kan dette skje dersom det er nødvendig for å ivareta den daglige driften eller andre berettigede interesser i *avdeling x* eller ved begrunnet mistanke om at dine handlinger er grovt brudd på dine plikter som følge av arbeidsforholdet eller kan gi grunnlag for oppsigelse eller avskjed**. Alt slikt innsyn vil foretas iht. lovens detaljerte regler om dette.**

1. **Kameraovervåkning**

*Dette må tilpasses i forhold til hvordan avdelingen har det.*

1. **kontaktinformasjon**

*Her må det framgå hvem som skal kontaktes for at man skal få utøvd sine rettigheter.*

Se for øvrig "Rutine - innsyn, retting og sletting".

**Vedlegg:**

* "Rutine – innsyn, retting og sletting"
* "Systemoversikt – ansatte og valgte i *avdeling xx*"
* "Skjema for krav om innsyn, retting eller sletting"



*Forslag til MAL 10*

# Personvernerklæring for medlemmer i avdeling x

(Organisasjonsnummer xxx)

**Sist oppdatert 26.04.2022**

[](http://www.google.com/url?sa=i&rct=j&q=&esrc=s&source=images&cd=&cad=rja&uact=8&ved=2ahUKEwjGq4zR6-7bAhWLhiwKHcIvDxgQjRx6BAgBEAU&url=http://www.abbl.no/Aktuelt/Ny-eierseksjonslov-tilbud-om-revisjon-av-boligsameiets-vedtekter&psig=AOvVaw2kYehQRsTl-e5X9zLNvJ6d&ust=1530016994152338)

1. **Innledning**

Avdelingsleder er behandlingsansvarlig[[7]](#footnote-7) for de personopplysninger vi har registrert og behandler i forbindelse med ditt medlemskap i avdeling x.  
  
Denne personvernerklæringen gir deg informasjon om hvordan vi behandler dine personopplysninger og hvilke rettigheter du har.

1. **Personopplysninger som avdelingen registrerer**

Må fylles ut

**2.1 Hva avdelingen bruker personopplysningene til**

Grunnlaget for behandling av personopplysninger er enten at behandlingen er nødvendig for å oppfylle forpliktelser knyttet til medlemskapet, at vi er pålagt behandlingen i lov eller at vi har en berettiget interesse i behandlingen som overskrider eventuell personvernmessig ulempe for deg.

Under angis de mest sentrale formålene personopplysningene brukes til:

Må fylles ut

1. **Hvem deler vi opplysningene dine med**

Må fylles ut

1. **Geografisk lagring av personopplysninger**

Må fylles ut

Eksempel:

*I utgangspunktet lagres ikke personopplysninger utenfor Norge, men enkelte driftsleverandører har driftssenter i EU hvor GDPR følges.*

1. **Hvor lenge lagrer vi opplysningene om deg**

*Avdelingen lagrer dine personopplysninger så lenge det er nødvendig, eller vi er pålagt lagring etter lov.*

1. **Dine rettigheter**

Personvernregelverket gir deg rettigheter knyttet til dine personopplysninger:

* Selv om denne personvernerklæringen gir mye informasjon, kan du be om mer inngående informasjon om hvordan vi behandler opplysninger om deg og du har rett til innsyn i dine personopplysninger. Dersom dine personopplysninger er feil, har du rett til å få dem rettet. Personopplysninger som vi eventuelt ikke har grunnlag for å behandle, skal slettes og du kan kreve dette gjort om vi ikke har sørget for dette på eget initiativ. Du kan også be om at vi begrenser bruk av dine opplysninger.
* Hvis du mener at vi behandler dine opplysninger uten rettslig grunnlag, kan du klage til Datatilsynet, men vi anmoder deg om å kontakte avdelingen slik at vi kan ta stilling til dine innvendinger og at vi kan oppklare eventuelle misforståelser.
* Dersom du ønsker å gjøre bruk av dine rettigheter henvender du deg til *avdeling x/person x* og din henvendelse vil, etter at personvernforordningen har tredd i kraft i Norge, bli besvart innen 30 dager. Se "Rutine – innsyn, retting og sletting" samt "Skjema for krav om innsyn, retting eller sletting".

1. **Kontaktinformasjon**

Forespørsel om innsyn, retting og sletting rettes til x

**Vi gjør oppmerksom på at det også finnes personopplysninger i Fellesforbundet.**



*Forslag til MAL 11*

# Databehandleravtale

mellom

**[Fellesforbundet avdeling xx]**

[Org.nr xx]

*Behandlingsansvarlig*

og

**[Leverandør]**

[Org.nr yy]

*Databehandler*

1. **Avtalens formål**

Partene har [*sett inn dato*] inngått en databehandleravtale.

Formålet med denne Databehandleravtalen er å regulere Partenes rettigheter og plikter, for derved å sikre at Personopplysningene behandles i overensstemmelse med de vilkår som følger av personopplysningsloven (lov av 15. juni 2018 nr. 38), personopplysningsforskriften (forskrift av 15. juni 2018 nr. 876) og EUs personvernsforordning 2016/679 og senere lovgivning som erstatter disse ("Personopplysningslovgivningen").

Målet med databehandleravtalen er å beskytte personopplysningene med hensyn til konfidensialitet, integritet og tilgjengelighet. Dette gjelder personopplysninger om ansatte, valgte og medlemmer av [Fellesforbundet avdeling XX].

Avtalen regulerer databehandlers behandling av personopplysninger på vegne av behandlingsansvarlig, herunder innsamling, registrering, sammenstilling, lagring, utlevering eller kombinasjoner av disse.

1. **Definisjoner**

**Personopplysninger**

Med personopplysninger menes opplysninger og vurderinger som kan knyttes til en enkelt person.

**Behandling**

Med behandling menes enhver bruk av personopplysninger, som f.eks. innsamling, registrering, sammenstilling, lagring og utlevering eller en kombinasjon av slike bruksmåter.

**Behandlingsansvarlig**

Med behandlingsansvarlig menes den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes.

**Databehandler**

Med databehandler menes den som behandler personopplysninger på vegne av den behandlingsansvarlige.

1. **Behandlinger**

Følgende personopplysninger behandles:   
Eks:

* fødsels- og personnummer
* fagforeningsmedlemskap
* opplysninger om ansatte (personalsaker i personalmappene)

Følgende behandlinger omfattes av denne avtalen:

* [List behandlinger som leverandør skal gjøre, eventuelt vis til vedlegg eller driftsavtale]

1. **Databehandlers plikter**

Databehandler skal overholde alle relevante bestemmelser i Personopplysningslovgivningen. Databehandler skal etablere tekniske og organisatoriske tiltak for å sikre at personopplysningene blir behandlet i tråd med personopplysningslovgivningen og vilkårene i denne databehandleravtalen. Tiltakene skal dokumenteres.

Databehandler skal følge de rutiner og instrukser som er avtalt ved inngåelsen av kontrakten.

Databehandler plikter å gi behandlingsansvarlig tilgang til sin sikkerhetsdokumentasjon, og bistå, slik at behandlingsansvarlig kan ivareta sitt eget ansvar etter lov og forskrift. Behandlingsansvarlig har, med mindre annet er avtalt eller følger av lov, rett til tilgang og innsyn i personopplysningene som behandles og systemene som benyttes til dette formål. Databehandler plikter å gi nødvendig bistand til dette.

Databehandler har taushetsplikt om dokumentasjon og personopplysninger som vedkommende får tilgang til iht. denne avtalen. Denne bestemmelsen gjelder også etter avtalens opphør.

Databehandler har ikke råderett til personopplysningene, og kan derfor heller ikke behandle disse til egne formål.

Databehandler skal ha på plass rutiner og systematiske tiltak for oppfølging av avvik, herunder tiltak for gjenoppretting av normal tilstand, fjerning av årsaken til avviket og hindre gjentakelse.

Databehandler skal uten ugrunnet opphold melde fra til behandlingsansvarlig om brudd på Personopplysningssikkerheten som har medført en hendelig eller ulovlig tilintetgjørelse, tap, endring, uautorisert utlevering av eller tilgang til personopplysningene.

Databehandler plikter å holde seg informert om eventuelle endringer i lovgivningen og det generelle risikobildet som kan ha betydning for denne avtalen og avtale nødvendige endringer.

1. **Behandlingsansvarliges plikter**

Behandlingsansvarlig skal straks melde fra til databehandler om forhold som vil kunne medføre behov for endringer i den måten databehandler behandler opplysningene på, herunder endringer i hvilke kategorier personopplysninger som inngår i behandlingen.

Behandlingsansvarlig plikter i samsvar med personvernforordningen innen rimelig tid å besvare forespørsler fra de registrerte eller tilsynsorganet om behandlingen som omhandles i denne avtalen.

Behandlingsansvarlig plikter å holde seg informert om eventuelle endringer i lovgivningen og det generelle risikobildet som kan ha betydning for denne avtalen og avtale nødvendige endringer.

1. **Bruk av underleverandører**

Dersom databehandler benytter seg av underleverandører eller andre som normalt ikke er ansatt hos databehandler, skal dette avtales skriftlig med behandlingsansvarlig før behandlingen av personopplysninger starter. En slik avtale gjøres som et tillegg til denne avtalen.

Samtlige som på vegne av databehandler utfører oppdrag der bruk av de aktuelle personopplysningene inngår, skal være kjent med databehandlers avtalemessige og lovmessige forpliktelser og oppfylle vilkårene etter disse.

1. **Sikkerhet**

Databehandler skal etablere tekniske og organisatoriske informasjonssikkerhetstiltak som står i et rimelig forhold til den risikoen Behandlingen representerer. Dette omfatter også tiltak for å sikre at personer som har autorisert tilgang til personopplysningene bare behandler disse i tråd med denne databehandleravtalen og behandlingsansvarliges instrukser. Tiltakene skal dokumenteres.

1. **Sikkerhetsrevisjoner**

Behandlingsansvarlig er ansvarlig for å gjennomføre sikkerhetsrevisjoner som kan omfatte gjennomgang av rutiner, stikkprøver, stedlige kontroller og eventuelle andre avtalte og egnede kontrolltiltak.

1. **Avtalens varighet, endring og opphør**

Avtalen gjelder fra den er signert av begge parter og så lenge databehandler behandler personopplysninger på vegne av behandlingsansvarlig.

Avtalen kan ikke endres på en slik måte at forutsetningen med behandlingen kommer i strid med formålet i denne avtalen. Ved endringer ut over formålet skal avtalen sies opp og ny inngås.

Behandlingsansvarlig kan ved brudd på denne avtalen eller på bestemmelsene i personopplysningsloven eller personopplysningsforskriften pålegge databehandler å stoppe den videre behandlingen av opplysningene med øyeblikkelig virkning. Behandlingsansvarlig kan ved brudd, si opp denne avtalen med minst 14 dagers varsel.

Ved opphør av denne avtalen plikter databehandler å tilbakelevere alle personopplysninger som er mottatt på vegne av den behandlingsansvarlige og som omfattes av denne avtalen. Alternativt skal databehandler slette alle dokumenter og forsvarlig destruere alle lagringsenheter som inneholder opplysninger som omfattes av avtalen. Dette gjelder også for eventuelle sikkerhetskopier.

Databehandler skal skriftlig bekrefte eller dokumentere at sletting og eller destruksjon er foretatt i henhold til avtalen innen rimelig tid etter avtalens opphør.

Alle kostnader som påløper ved opphør av avtalen dekkes av behandlingsansvarlig forutsatt at databehandler har oppfylt sine forpliktelser i henhold til denne avtalen.

1. **Meddelelser**

Meddelelser etter denne avtalen skal sendes skriftlig til:

|  |  |
| --- | --- |
| [Leverandør] | [Fellesforbundet avdeling xx] |
| [Kontaktperson] | [Kontaktperson] |
|  |  |

1. **Lovvalg og verneting**

Avtalen er underlagt norsk rett og partene vedtar Oslo tingrett som verneting. Dette gjelder også etter opphør av avtalen.

\*\*\*

Denne avtalen er i to eksemplarer hvorav partene beholder hvert sitt eksemplar.

Sted og dato Sted og dato

…………………………………….. …………………………………………..

For [Leverandør] For [Fellesforbundet avdeling xx]



*Forslag til MAL 12*

# Avviksrapportering

**1. Innledning**

Formålet med avviksrapportering er å avdekke uønskede hendelser slik at det er mulig å komme med korrigerende tiltak for å unngå gjentakelser.

**2. Hva er et avvik / brudd på personopplysningssikkerheten**

Et brudd på personopplysningssikkerheten, er et brudd på sikkerheten som fører til utilsiktet eller ulovlig tilintetgjøring, tap, endring, ulovlig spredning av eller tilgang til person-opplysninger som er overført, lagret eller på annen måte behandlet.

Dette kan kategoriseres i:

1. **Brudd på konfidensialitet**, det vil si at det har vært en utilsiktet eller ulovlig utlevering av, eller tilgang til, personopplysninger.
2. **Brudd på integritet**, det vil si at det har vært en utilsiktet eller ulovlig endring av personopplysninger.
3. **Brudd på tilgjengelighet**, det vil si at det har vært et utilsiktet eller ulovlig tap av tilgang til, eller tilintetgjøring av, personopplysninger.

Et brudd kan omfatte en, eller en kombinasjon av disse tre. Det avhenger av omstendighetene.

**3. Hvordan håndteres avvik**

Avvik skal forsøkes rettet umiddelbart og på lavest mulig nivå i organisasjonen. Rapportering av avvik skal skje fortløpende til ………

…….. registrerer avvikene i et internt avvikshåndteringssystem. …… vurderer innmeldte avvik og iverksetter nødvendig tiltak. Om nødvendig vil ……. melde avvik videre til Datatilsynet.

**4. Når skal avvik meldes til Datatilsynet (risiko: middels og høy)**

Ved brudd på personopplysningssikkerheten skal den behandlingsansvarlige uten ugrunnet opphold og når det er mulig, senest 72 timer etter å ha fått kjennskap til det, melde bruddet til Datatilsynet, med mindre bruddet sannsynligvis ikke vil medføre en risiko for fysiske personers rettigheter og friheter. Dersom bruddet ikke meldes til tilsynsmyndigheten innen 72 timer, skal årsakene til forsinkelsen oppgis.

Når er det nødvendig å informere de berørte? (risiko: høy)

Dersom det er sannsynlig at bruddet på personopplysningssikkerheten vil medføre høy risiko for fysiske personers rettigheter og friheter, skal den behandlingsansvarlige uten ugrunnet opphold underrette den registrerte om bruddet.

**5. Hvordan vurdere risiko**

Med en gang man er klar over at det har skjedd et brudd, skal man håndtere og begrense det, men man må samtidig avgjøre hvilken risiko det kan ha medført for de som er berørt av bruddet.

* Dersom det er ingen eller lav risiko, er det ikke behov for å melde fra til Datatilsynet eller til de berørte.
* Dersom det er middels risiko, er det nødvendig å melde fra til Datatilsynet, men ikke informere de berørte.
* Dersom det er høy risiko, er det nødvendig å melde fra til Datatilsynet og informere de berørte.

Når man skal vurdere risiko av et brudd må man se på de konkrete omstendighetene rundt et brudd, herunder dens alvorlighetsgrad og potensielle innvirkning. For å avgjøre dette kan man se på følgende kriterier som må vurderes mot hverandre:

* Hva slags type brudd er det:  
  Her må man vurdere om det er brudd på konfidensialitet, integritet eller tilgjengelighet.
* Personopplysningenes art, sensitivitet og mengde
* Hvor lett er det å identifisere enkeltpersoner
* Alvorlighetsgrad av konsekvenser for enkeltpersoner:  
  Her må man se på hva bruddet kan medføre for den enkelte. Hvor lett er det at bruddet kan føre til ID-tyveri eller svindel, fysisk skade, psykisk påkjenning, ydmykelse eller skade på omdømme.
* Spesielle egenskaper ved enkeltpersoner:  
  Et brudd som omfatter personopplysninger om barn eller andre sårbare enkeltpersoner eller utsatte grupper, kan medføre større konsekvenser for dem.
* Antall berørte enkeltpersoner

**6. Eksempler på avvik som skal meldes**

Som hovedregel skal alle hendelser som får eller kunne fått uheldige menneskelige, økonomiske eller omdømmemessige konsekvenser rapporteres.

Alle avvik i forhold til sikkerhet registreres i avdelingens avvikshåndteringssystem og meldes til Datatilsynet når risikoen er vurdert til middels eller høy.

Eksempler:

**Forsendelsesfeil**

* Beskyttelsesverdige personopplysninger er sendt til feil mottaker pr. post eller e-post.
* Digitale forsendelser som avslører andres e-postadresse i en kontekst hvor mottakeren skal beskyttes.
* Forsendelser til riktig mottaker, men som ved en feil også inneholder beskyttelsesverdige personopplysninger om andre.
* Postforsendelser til riktig mottaker, men hvor det er informasjon om mottakeren som skal skjermes for andre er synlig utenpå forsendelsen.
* Postforsendelser hvor inneholder mangler eller innholdet er der, men konvolutten er revet opp.

**Hacking eller datainnbrudd**

Personopplysninger har blitt hentet ut, er endret på eller er utilgjengelig, eller at det er sannsynlig at dette har skjedd.

**Tilgangsstyring feilet, er mangelfull eller manglende**

Uvedkommende har fått tilgang til beskyttelsesverdige personopplysninger.

**Nettpublisering av personopplysninger**

Opplysningene skulle ikke har vært publisert eller personopplysningene har ikke blitt anonymisert.

**Fysisk innbrudd**

Ukrypterte digitale data eller papirdokumenter med personopplysninger er forsvunnet.

**Kaste/kvitte seg med opplysninger uten sletting eller makulering**

**Mistet/gjenglemt/forlagt**

* Papirdokumenter
* Laptop, nettbrett eller telefoner der innholdet ikke er kryptert
* Minnepinner eller andre små lagringsmedier der innholdet ikke er kryptert
* Nøkler og adgangskort

**Vedlegg:**

Skjema for avviksrapportering



**Avviksskjema**

**Dato**:

|  |  |
| --- | --- |
| **Hvem** rapporterer: |  |

|  |  |
| --- | --- |
| **Hva** gjelder det: |  |

Er hendelsen rapportert til overordnet leder? JA  NEI

|  |
| --- |
| **Beskrivelse av hendelsen**: |

|  |
| --- |
| **Hva er gjort for å rette feilen/hindre gjentakelse:** |

|  |
| --- |
| Annet: |

**Skjemaet skal sendes sikkerhetsansvarlig/……**

|  |
| --- |
| **Kommentar fra sikkerhetsansvarlig/……….**: |

1. Behandlingsansvarlig er den som bestemmer formålet med behandlingen med personopplysninger og hvilke hjelpemidler som skal benyttes, ref. personvernforordningens artikkel 4, pkt. 7 [↑](#footnote-ref-1)
2. Behandlingsansvarlig er den som bestemmer formålet med behandlingen med personopplysninger og hvilke hjelpemidler som skal benyttes, ref. personvernforordningens artikkel 4, pkt. 7 [↑](#footnote-ref-2)
3. Det er svært viktig at avdelingen verifiserer at det er riktig person man utgir personopplysninger til. [↑](#footnote-ref-3)
4. Behandlingsansvarlig er den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal benyttes, ref. personvernforordningens artikkel 4, pkt. 7 [↑](#footnote-ref-4)
5. Databehandler er en fysisk eller juridisk person som behandler personopplysninger på vegne av den behandlingsansvarlige, ref. personvernforordningens artikkel 4. pkt. 8. [↑](#footnote-ref-5)
6. GDPR: General Data Protection Regulation. (EUs personvernforordning) [↑](#footnote-ref-6)
7. Behandlingsansvarlig er den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal benyttes, ref. personvernforordningens artikkel 4, pkt. 7 [↑](#footnote-ref-7)