Personvern

Guide fra Frivillighet Norge

Hva er GDPR?

General Data Protection Regulation(GPDR) tok over for Personopplysningsloven i 2018. Den gjelder for alle virksomheter i EU og EØS.

Personvern handler om retten til å ha et privatliv og retten til å bestemme over egne personopplysninger. For oss som frivillige organisasjoner handler det om at medlemmer og samarbeidspartnere skal kunne ha tillit til oss og hvordan vi behandler deres persondata.

Den nye forordningen betyr flere rettigheter for forbrukeren og flere plikter for organisasjonen. Alle som jobber, er tillitsvalgte eller frivillige i en organisasjon og som håndterer personopplysninger, må nå forholde seg til flere regler for dette.

Datatilsynet er ansvarlig for å føre tilsyn og håndheve loven i Norge. De har gjort tilgjengelig dokumenter og ressurser som gjelder den nye forordningen på sine nettsider. Dette er imidlertid store mengder informasjon, som ikke er målrettet mot enkelte bransjer.

Denne guiden er til frivillige organisasjoner.

FRIVILLIGHET NORGE

Sjekkliste:
Åtte steg til et godt personvern

1. Har dere en oversikt over alle persondataene dere behandler?
2. Har dere skrevet ned og dokumentert rutinene deres?
3. Har dere slettet alle persondata dere ikke trenger?
4. Har dere rutiner for å innhente samtykke for de persondataene dere behandler?
5. Har dere forenklet språket på informasjon dere gir til medlemmer/ publikum?
6. Har dere laget en personvernerklæring som ligger lett tilgjengelig på nettsiden deres?
7. Har dere laget avtaler med databehandlerne dere bruker?
8. Har dere laget en årsplan for gjennomgang av rutiner og risikovurdering av arbeidet med personopplysninger i organisasjonen?

Et bra sted å starte - forankring i organisasjonen

Den nye forordningen er ikke et nytt IKT-prosjekt. Å forankre og implementere de nye reglene er et ansvar på ledernivå og bør behandles på styrenivå slik at man sikrer nok ressurser til arbeidet i organisasjonen. Jo flere i organisasjonen som inkluderer personvern i daglige rutiner, jo enklere og raskere vil dere komme inn i et godt spor for arbeidet med personvern.

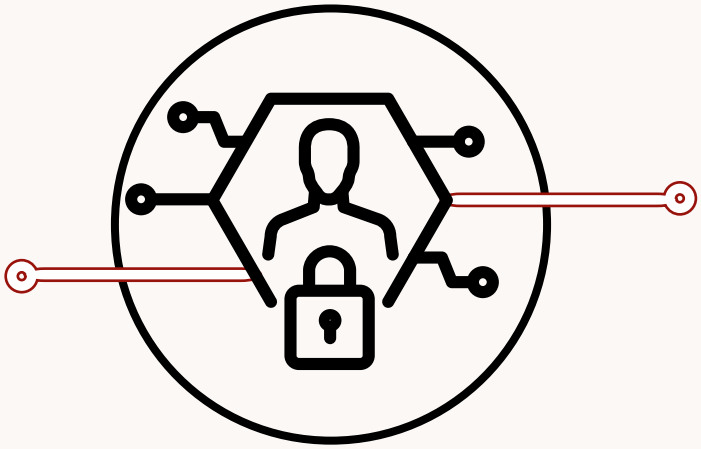
KNAPPE RESSURSER? HVEM DELTAR?

Mange frivillige organisasjoner har få ansatte og flere baserer seg i stor grad på frivillige ressurser og tillitsvalgte. Uansett størrelse på organisasjonen deres og om driften er basert på frivillige eller ansatte, vil vi anbefale dere å sette sammen en gruppe som leder arbeidet med kartlegging og sikrer framdriften på arbeidet med personvern.

Når det gjelder gruppesammensetning og hvem som er med: Det er viktigere med interesse og motivasjon for å arbeide med personvern, enn en spesifikk kompetanse på de som er med i gruppen.

WORKSHOP?

For å sette fokuset på viktigheten av å jobbe godt med personvern i hele organisasjonen, vil vi anbefale å sette av tid til en stabsdag/workshop som gir en innføring i hva som blir nytt med det nye regelverket og hva dette betyr for deres organisasjon. En slik samling gjør det enklere å stake ut kursen i arbeidet med å gjøre organisasjonen klar for det nye regelverket.



Grunnleggende begreper

En personopplysning er enhver opplysning som kan knyttes til en fysisk person. For eksempel: navn, alder, e-post adresse, postadresse, IP-adresse, bilnummer, bilder, lønn og opplysninger om atferdsmønster.

En sensitiv personopplysning er opplysninger om en persons helse, religiøs tilknytning, politisk tilknytning, seksuell legning eller et fagforeningsmedlemskap. Sensitive personopplysninger har strengere krav til behandling og oppbevaring enn det vanlige personopplysninger har. Religiøse organisasjoner, politiske organisasjoner og interesseorganisasjoner for helse, behandler sensitive personopplysninger gjennom persondata om sine medlemmer.

Behandling av persondata er all bruk og håndtering av personopplysninger, for eksempel til innsamling, registrering, lagring og utlevering.

Registre er alle former for strukturerte samlinger av persondata som medlemsregister, adresselister, lister over frivillige, ansattlister, deltakerlister osv.

Et samtykke må som regel foreligge før man bruker en personopplysning til noe. Samtykket skal være en frivillig, spesifikk og utvetydig erklæring om at den registrerte aksepterer behandlingen som blir gjort av personopplysningene.

Behandlingsansvarlig er organisasjonen som håndterer personopplysninger. Det er organisasjonen som bestemmer formålet med behandlingen og hvordan det skal gjøres.

En databehandler er den som behandler persondata på vegne av den behandlingsansvarlige (organisasjonen) og som dermed kan få innsyn i personopplysninger. Eksempler på en databehandler kan være en leverandør av medlemsregisteret dere bruker, IT-drift, regnskapsprogrammet eller personaladministrasjon.

I forkant av at det nye regelverket trer i kraft må det inngås **databehandleravtaler** med hver av leverandørene dere bruker.

Et avvik forekommer når personopplysninger behandles feil i forhold til fastlagte rutiner eller det er mistanke om brudd på informasjonssikkerhet.

Ansatte og frivillige
- rutiner og informasjonssikkerhet

Grunnleggende sikkerhet og gode rutiner for personvern starter med den enkelte ansatte i organisasjonen. Dette er rutiner som bidrar til at personopplysninger ikke kommer på avveie.

PASSORD

- Passord er personlig og deles ikke med andre.
- Kombiner tall, små og store bokstaver.
- Passordet bør ha minst seks tegn.
- Bytt passord regelmessig.

E-POST

- Bruk blindkopi/bcc ved distribusjon av e-post der det er flere mottakere som ikke skal være kjent for hverandre.
- Sensitive personopplysninger skal ikke sendes pr e-post.
- Lister med personopplysninger sendes ikke som vedlegg, men med lenker.
- Om du mottar sensitive personopplysninger på e-post, skriv ut e-posten, slett den og behandle e-posten i tråd med innholdet.

MOBIL

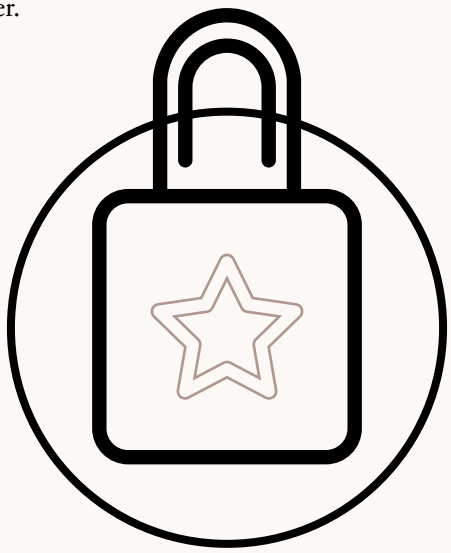
- Ha passord på åpning av skjerm og ved oppstart av mobiltelefonen.

BÆRBAR PC

- Logg ut når du ikke arbeider på maskinen.
- Ikke lagre sensitive personopplysninger på PC, minnepinne eller mobiltelefon.

SIKKERHET PÅ KONTORET

- Sørg for trygg oppbevaring av nøkler, adgangskort og passord.
- Pass på elektronisk utstyr og sørg for at uvedkommende ikke får tak i informasjon og utstyr.
- Ha gode rutiner for å ta i mot besøkende.
- Følg opp evt. uvedkommende og uventet besøk.
- Lås inn sensitive personopplysninger.



Personvernerklæring

Personvernerklæringen skal beskrive de områdene i organisasjonen hvor dere håndterer personopplysninger sammen med en beskrivelse av rutinene rundt disse. Språket i erklæringen skal være forståelig og tilgjengelig for den som leser. Også for barn, om de er en del av målgruppen.

I erklæringen må det også komme fram hvor man kan henvende seg for å få slettet eller endret personopplysningene sine.

Personvernerklæringen skal ligge lett tilgjengelig og synlig på nettsiden deres. Den skal beskrive alle sammenhenger og på hvilke måter persondata håndteres. Eksempel på personvernerklæring for frivillig organisasjon

Et samtykke er et av flere likestilte behandlingsgrunnlag som må foreligge før man bruker en personopplysning til noe. Samtykket skal være en *frivillig, spesifikk og utvetydig* erklæring om at personen aksepterer behandlingen som blir gjort med personopplysningene av organisasjonen.

Et samtykke gjelder til det blir trukket tilbake. Man kan også gi samtykke som gjelder for en viss periode. I slike tilfeller gjelder ikke samtykket når perioden er over.

RUTINER FOR INNHENTING

Uansett må dere lage rutiner for innhenting av samtykke og vi anbefaler å bruke de anledningene som byr seg i møte med medlemmer og givere. For eksempel vil en digital utsendelse til alle medlemmer kunne inneholde et samtykkeskjema for noe som skal skje fram i tid.

FORSTÅELIG OG TILGJENGELIG INFORMASJON

Det må gis tilstrekkelig med informasjon om hva som skal gjøres med personopplysningene til den det angår. Dette gjøres i en personvernerklæring, og i den øvrige skriftlige informasjonen som gis i forbindelse med inngåelse av et samtykke. I den nye forordningen er det økt krav til informasjonen som blir gitt: Den skal være forståelig og tilgjengelig for mottakeren. Skriftlig informasjon til barn skal tilpasses barnets forståelsesnivå.

SAMTYKKE

«Take it or leave it»- samtykker er ikke lenger tillatt. Samtykkende må være nyanserte og man samtykker aktivt for ulik bruk.

Eksempel:

Jeg samtykker i å

- ☐ Motta informasjon om arrangementer
- ☐ Motta nyheter pr. epost
- ☐ Motta påminnelser på sms
- ☐ Fotografering under frokostseminaret

EKSEMPEL PÅMELDING ARRANGEMENT

Velkommen til vår maikonferanse 2019! Meld deg på her:

Navn:
Adresse:
Epost:
Telefon:

- ☐ Har du allergier eller andre behov vi skal ta hensyn til?
- ☐ Personopplysningene du oppgir blir brukt og lagret for dette arrangementet. Om du ønsker å motta informasjon om framtidige arrangementer i regi av oss kryss her.

Organisasjonens navn vil ta bilder under <navn på arrangement>. Bildene vil bli brukt i sosiale nettsaker og pressesaker som omhandler arrangementet og eventuelt andre publikasjoner som omhandler <arrangement> i regi av <organisasjonens navn>. Er det greit at vi bruker disse bildene?

- ☐ Ja, det er greit at bilder av meg blir brukt i denne sammenhengen.

Dokumentér, dokumentér, dokumentér!

Om Datatilsynet kommer på besøk og gjennomfører tilsyn hos dere, vil å se hva slags rutiner dere har for håndtering og oppbevaring av persondata. Da holder det ikke at én person i organisasjonen kan ramse opp noen rutiner fra sitt eget hode. Alt dere har av rutiner må være begrunnet og skrevet ned.

Når dere tar en **full gjennomgang** av persondataene, er det naturlig å fortsette arbeidet med å gå gjennom og skrive ned rutinene dere har for alle persondata dere håndterer i organisasjonen. Her følger noen eksempler på spørsmål dere kan stille ved en slik gjennomgang:

EKSEMPEL 1 - MEDLEMSREGISTERET

- Hvem har tilgang til medlemsregisteret?
- Hvem trenger tilgang til hva?
- Hvem kan hente ut rapporter/lister?
- Vedkommende må kjenne rutinene for hva man kan gjør med listene.
- Oppbevaring/håndtering/sletting av opplysninger fra medlemsregisteret.
- Databehandler - egen avtale må inngås.

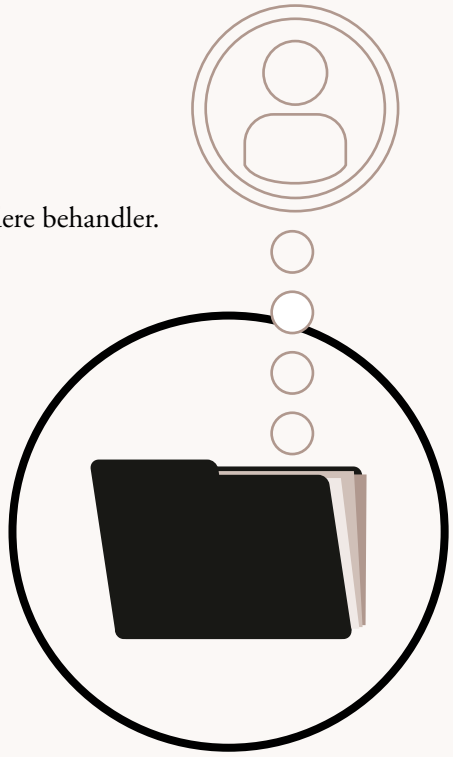
EKSEMPEL 2 - ANSATTINFORMASJON

- Hvem har tilgang til denne informasjonen?
- Hvor lagres opplysningene?
- Hvilken informasjon er nødvendig å ha?
- Når slettes opplysninger over tidligere ansatte?
- Hvilke opplysninger beholdes og hvorfor?

EKSEMPEL 3 - AVVIK

- Hvordan håndteres avvik i organisasjonen?
- Hvordan dokumenteres avvikene?
- Hvordan følges de opp internt?
- Hvem er ansvarlig for å følge opp og melde til Datatilsynet?

Samme spørsmål stilles og dokumenteres knyttet til alle persondataene dere behandler.

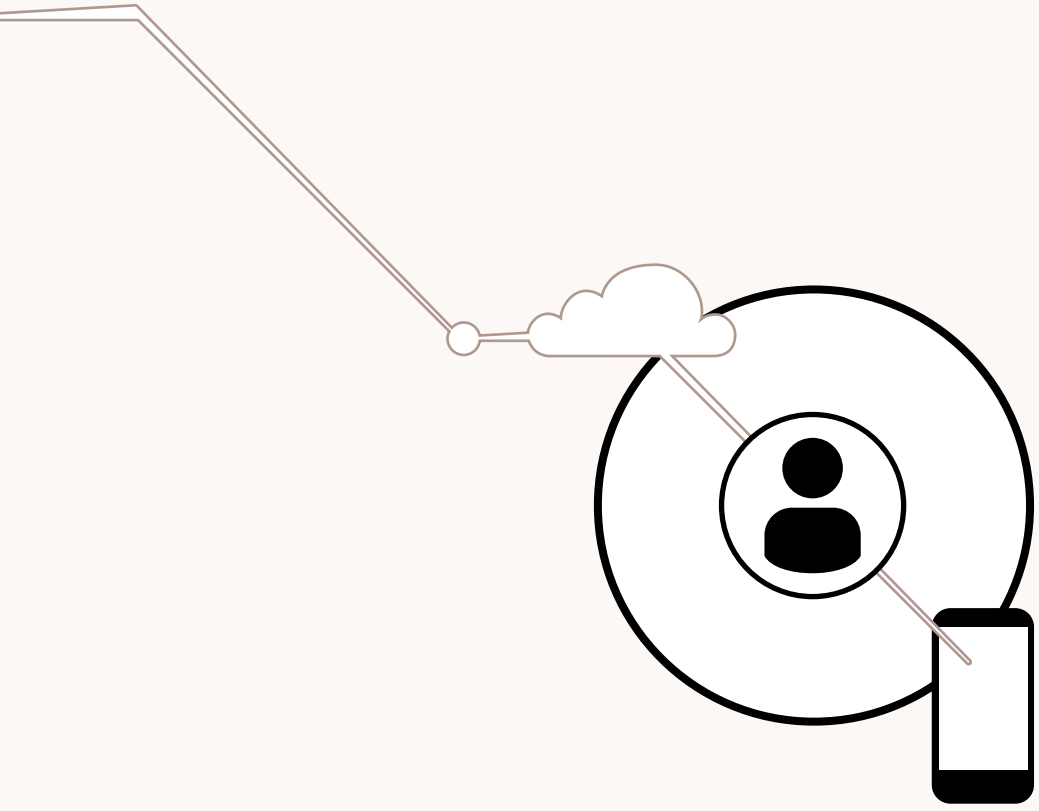


Håndtering av lister

Når personopplysningene er innhentet og trygt lagret i medlemsregisteret eller annen database, har man som regel god sikkerhet rundt dataene. Ofte har man imidlertid behov for å ta ut lister og rapporter til bruk i organisasjonen, enten elektronisk som en fil eller i form av en fysisk rapport, på papir. Da er det større risiko for at personopplysninger kan komme på avveie. Da er det avgjørende å ha gode rutiner for hvilke lister man behandler, hvem som gjør det og hvordan de håndteres.

VIKTIGE PRINSIPPER FOR HÅNDTERING AV LISTER

- Har personene som håndterer personopplysninger hos dere underskrevet taushetserklæring?
- Hvem har tilgang til medlemsregisteret, og hvem kan gjøre hva med hvilke personopplysninger? Prinsippet bør være at kun de som trenger tilgang, får tilgang og kun til de personopplysningene vedkommende trenger.
- Hvem får tilgang til opplysningene man henter ut?
- Har dere utarbeidet rutiner for håndtering/oppbevaring av lister?
- Listene slettes/makuleres så snart de ikke er i bruk.
- Passord på kopimaskinen sikrer at lister og opplysninger ikke kommer på avveie.
- Sensitive opplysninger bør ikke sendes på e-post. Om nødvendig bør man sende de som vedlegg i form av lenke.
- Lister med sensitive opplysninger må oppbevares i låsbare skap.



Bilder - tagging og sporing

Med den digitale tiden vi lever i, og med den lette tilgangen vi har til bilder, bruker frivillige organisasjoner visuell kommunikasjon mer enn noen gang.

Ved fotografering av mennesker må det innhentes samtykke for bruk av bildene. Her er det viktig å lage rutiner for å hente inn samtykke i forkant av at bilder blir tatt og publisert, og hvor den enkelte aktivt samtykker i å bli fotografert og i at bilder kan gjengis og vises offentlig.

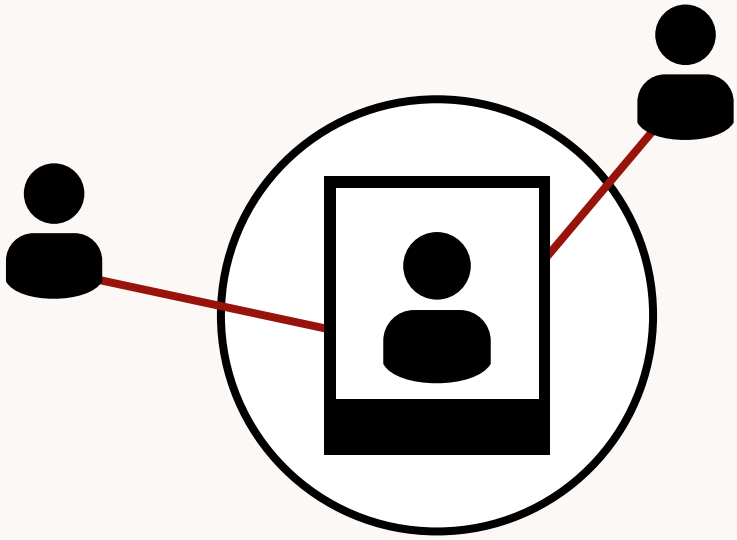
DET FINNES NOEN UNNTAK I ÅNDSVERKSLOVEN § 45C

Fotografi som avbilder en person kan ikke gjengis eller vises offentlig uten samtykke av den avbildede, unntatt når
a) avbildning har aktuell og allmenn interesse,
b) avbildningen av personen er mindre viktig enn hovedinnholdet i bildet,
c) bildet gjengir forsamlinger, folketog i friluft eller hendelser som har allmenn interesse,
d) eksempler av avbildningen på vanlig måte vises som reklame for fotografens virksomhet og den avbildede ikke nedlegger forbud eller
e) bildet brukes som omhandlet i § 23 tredje ledd eller § 27 andre ledd.
Vernet gjelder i den avbildedes levetid og 15 år etter hans dødsår.

TAGGING AV BILDER

Etter at et samtykke er innhentet, vil det være nødvendig å lage et system for å tagge og spore bilder. Dette vil si at dere har en database over hvem som er fotografert når, og hvor bilder av vedkommende er publisert. Dette er nødvendig fordi en person kan be dere slette personopplysninger dere har på vedkommende og det gjelder også bilder. Da er det nyttig å ha gode rutiner for å kunne spore hvor bilder er brukt.

Lov om opphavsrett til åndsverk mv. (åndsverkloven)



Retten til å bli glemt - sletting av data

Dere har ikke lov til å oppbevare personopplysninger «sånn i tilfelle» dere skulle får bruk for de en gang. Dette betyr at dere må slette personopplysninger dere ikke bruker eller som dere ikke har samtykke til å oppbevare.

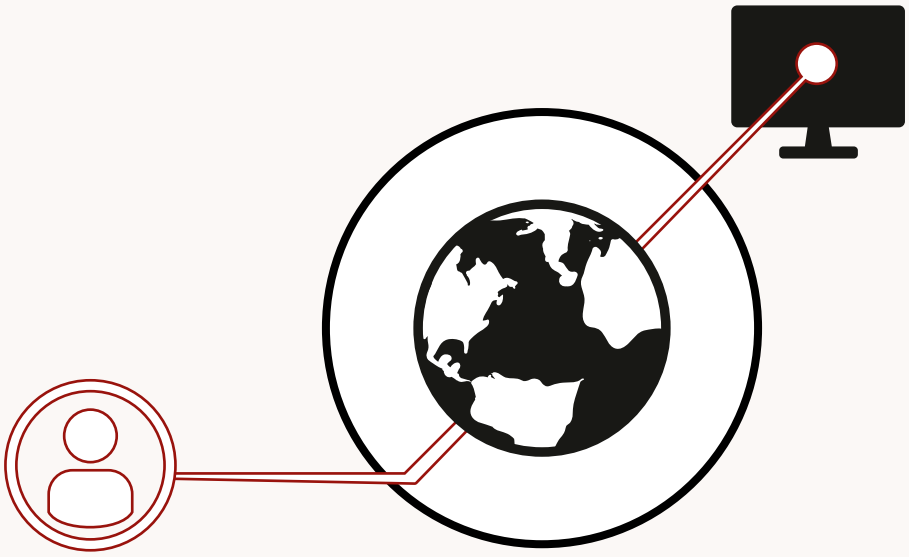
Nytt med forordningen er at et medlem eller giver har rett til å bli slettet i alle registre når det selv ønsker. En slik henvendelse skal følges opp med en gang og innen en måned.

- Er det slik at et *aktivt medlem* ønsker å bli slettet, kan dere som organisasjon ta vare på data knyttet til medlemskapet for å kunne dokumentere grunnlag for offentlig støtte i antall medlemmer. Medlemmet må da slettes fra det ordinære medlemssystemet og lagres eget sted, i tilfelle kontroll.
- Opplysninger i medlemsregisteret tilbake i tid kan være interessante å ha av historisk interesse, men persondataene må da anonymiseres om de skal beholdes. Fullt navn, adresse og fødselsdato på et medlem endres i slike tilfeller til kjønn og hvilket årstall vedkommende er født. På den måten er det fortsatt mulig å lage statistikk på gamle medlemslister, men uten at noen personer er identifiserbare.
- Mange frivillige organisasjoner har en lang og interessant historie. Av den grunn har vi bedt Arkivverket bistå oss med å utarbeide kjøreregler som kan brukes som grunnlag når historisk interesse skal vurderes opp mot hensynet til personvern.
- Ansatthistorikk - hva kan man beholde? Vi jobber med å innhente mer informasjon om dette.

Retten til å ta med seg persondata - dataportabillitet

Fra mai 2018 vil en registrert person kunne be om å ta med seg sine persondata for videre bruk i en annen sammenheng. Denne rettigheten gjelder kun opplysninger som den registrerte har avgitt eller som er samlet inn fra den registrerte og der hvor behandlingsgrunnlaget er et samtykke eller nødvendig for å gjennomføre en avtale.

Dette vil si at den data organisasjonen har om vedkommende samles i én fil og i det formatet som best kan tas med og brukes videre av andre.



Personvern og barn

En problemstilling som av og til melder seg, er behovet for samtykke fra foresatte når en rekrutterer medlemmer under 18 år. Det er ingen minstealder for organisasjonsmedlemskap, så en generell minstealder for medlemskap må vurderes etter hvilke aktiviteter organisasjonen tilbyr.

I dagens regelverk er hovedregelen at foreldre gir samtykke for barn under 15 år.

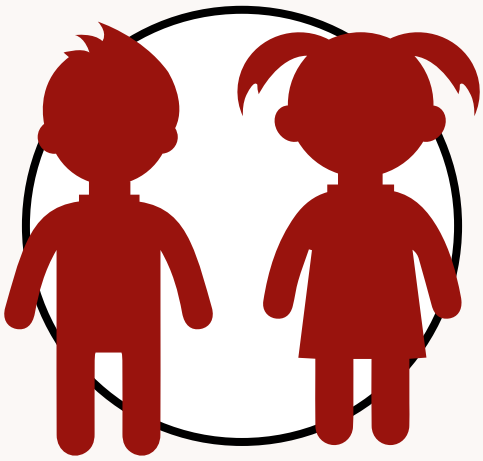
Et samtykke gjelder til det blir trukket tilbake. Dette gjelder både fra den mindreårige og den foresatte. Den mindreårige kan trekke tilbake samtykket selv om den foresatte opprinnelig samtykket til behandlingen. Opplysningene om barnet skal alltid slettes når samtykket er trukket tilbake.

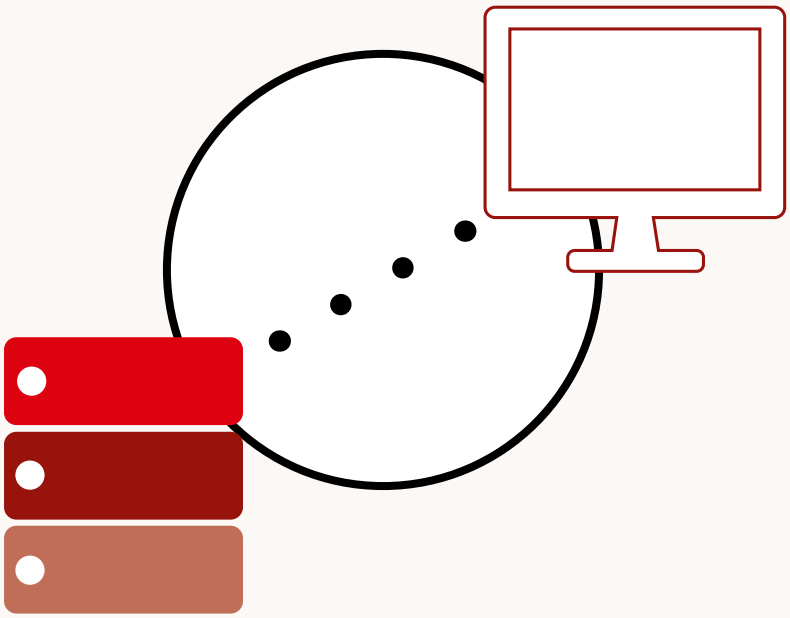
Barnet skal gjøre et frivillig og informert samtykke. Det betyr at informasjon som blir gitt i forbindelse med samtykke og personvernerklæringer rettet mot barn, skal tilpasses barnets alder.

Noen organisasjoner har egne aldersgrenser for demokratiske rettigheter i organisasjonen. Det er opp til organisasjonen selv om den ønsker å gi demokratiske rettigheter til mindreårige medlemmer, eller om den vil benytte en egen aldersgrense for stemmerett på årsmøtet eller for å kunne stille til valg.

Ifølge Barneombudets rettighetsplakat skal det legges stor vekt på det en mener i personlige forhold fra 12 år, og en har rett til å si sin mening om innmelding og utmelding av trossamfunn, mens barn fra 15 år har rett til å melde seg inn og ut av foreninger og trossamfunn.

En bør derfor vurdere å be om foreldrenes samtykke dersom en skal rekruttere medlemmer under 15 år og hvert fall for medlemmer under 12 år. Behovet for å innhente foreldrenes samtykke til medlemskap må også sees i sammenheng med størrelsen på medlemskontingenten foreningen krever. Jo høyere medlemskontingent, jo større oppfordring har foreningen til å innhente foreldrenes samtykke når barn melder seg inn.





Personvern skal bygges inn i nye løsninger

Datatilsynet anbefaler alle virksomheter som behandler personopplysninger eller som lager nye IKT-systemer om å følge prinsippene om innebygget personvern. Eksempler på nye IKT-systemer er apper og nettsider dere skal utvikle. Dette betyr at den tekniske løsningen blir laget slik at personvernet blir ivaretatt. Når forordningen trer i kraft blir dette en plikt. Som en del av kravet skal dere bruke personvern som standardinnstilling. Det betyr at det minst personverninngripende alternativet skal være standarden i alle systemer og løsninger.

I vurderingen av hvor personvernvennlige tiltakene kan gjøres, skal dere ta hensyn til tilgjengelig teknologi, implementeringskostnader, hvor omfattende de er og i hvilke sammenhenger de skal gjøres.

MAN SKAL HA STANDARDINNSTILLINGER FOR

- Mengden personopplysninger man samler inn.
- Omfang av behandlingen av personopplysninger.
- Lagringstid.
- Tilgjengelighet. Personopplysningene skal være tilgjengelig for det formålet som var tiltenkt.
- Det stilles også et krav om at det ikke skal være mulig å gjøre personopplysninger tilgjengelig for et ubestemt antall personer uten den registrertes medvirkning.

Datatilsynets syv steg til innebygd personvern

Databehandlere og krav til avtalen

Databehandlere behandler persondata på vegne av dere som organisasjon. Eksempler på databehandlere er regnskapssystemet dere bruker, medlemsregisteret og leverandør av løsning på nyhetsbrev.

Databehandlere er pliktige til å sørge for informasjonssikkerhet i måten de jobber på. De plikter også å varsle dere som oppdragsgivere (behandlingsansvarlige) om avvik. De må også opprette personvernombud om dere som organisasjon er pålagt det.

Selv om databehandlerne får nye plikter gjennom den nye forordningen, er det fortsatt dere som behandlingsansvarlige som har hovedansvaret for behandlingen av personopplysninger.

Det er viktig å få en avtale med databehandlere. Mange av de store databehandlerne (leverandørene) har laget standard databehandleravtaler som dere kan bruke som et utgangspunkt.

HVA MÅ MED I DATABEHANDLERAVTALEN?

- Databehandler skal kun behandle personopplysninger etter dokumenterte instruksjoner fra den behandlingsansvarlige (organisasjonen).
- Databehandler skal kun overføre personopplysninger til et land utenfor EU/EØS-området eller til internasjonale organisasjoner slik det er beskrevet i dokumenterte instruksjoner fra den behandlingsansvarlige.
- De som har tilgang til personopplysningene som behandles er underlagt taushetsplikt.
- Databehandler skal sørge for informasjonssikkerhet i tråd med artikkel 32.
- Databehandler må respektere reglene for underleverandører i tråd med artikkel 28.
- Avtalen skal spesifisere hvordan databehandler skal bistå den behandlingsansvarlige med å etterkomme krav fra enkeltpersoner.
- Avtalen skal spesifisere hvordan databehandler skal bistå den behandlingsansvarlige med informasjonssikkerhet, avvikshåndtering og konsekvensanalyse.
- Databehandler skal avhengig av hva den behandlingsansvarlige velger, slette eller tilbakeføre alle personopplysninger når databehandlingstjenestene opphører. Kopier skal også slettes. Dette gjelder med mindre en annen lov krever at de skal tas vare på.
- Databehandleravtalen skal være skriftlig og elektronisk.

UNDERLEVERANDØRER

Ofte har databehandlere underleverandører. En underleverandør er en leverandør av tekniske løsninger som behandler personopplysninger på vegne av databehandlerne.

Forordningen understreker at behandlingsansvarlig (organisasjonen) skal godkjenne alle underleverandører skriftlig. Forholdet mellom databehandleren og underleverandøren skal reguleres i en egen avtale mellom den behandlingsansvarlige og databehandleren, tilsvarende databehandleravtalen.

Rutiner ved avvik

Det at dere ikke har registrert noen avvik i arbeidet med personvern, er ikke nødvendigvis bra. Rutiner for å registrere og melde avvik viser at en organisasjon har gode rutiner og vet hva som er riktig og gal håndtering av personopplysninger.

Lovverket sier at avvik skal meldes Datatilsynet innen 72 timer. Samtidig må dere ta en gjennomgang av avviket, hvor og hvorfor feilen skjedde og hvordan dere skal bedre rutinene for å unngå at sammen feilen skjer igjen. I visse tilfeller må berørte personer varsles om avviket.

ETTER DE NYE REGLENE SKAL EN AVVIKSMELDING TIL DATATILSYNET INNEHOLDE

1. Beskrivelse av avviket, hvilke personer og personopplysninger som er berørt.
2. En oversikt over hvor mange personer/personopplysninger som er berørt.
3. En beskrivelse av hvilke konsekvenser avviket trolig vil ha.
4. En beskrivelse av hva dere vil gjøre for å «lukke» avviket og begrense konsekvensene av det.
5. Kontaktperson i organisasjonen.

EKSEMPLER PÅ AVVIK

- Skjema med helseopplysninger om alle speiderne i en speidergruppe forsvinner på leir.
- En liste med oversikt over ulike allergier hos påmeldte til kurs til helgens arrangement blir liggende på kopimaskinen hele dagen.
- Ansattes bærbare PC blir stjålet.

Skjema for melding om avvik på Altinn (DPA-01)

Personvernombud

Organisasjoner av en viss størrelse eller som behandler større mengder sensitive data, bør ha et personvernombud. Det er ikke satt en grense hvor skillet går for om dette er noe man må ha eller ikke.

Datatilsynet har imidlertid uttalt at de organisasjonene som har personvernombud, får et større fokus og mer kunnskap rundt arbeidet med personvern. Dette kan gjøre organisasjonen bedre rustet til å arbeide med personvern i alle ledd. Dersom det ikke opprettes personvernombud bør dere dokumentere de vurderingene dere har gjort, med mindre det er helt opplagt at dere ikke har en slik plikt.

PERSONVERNOMBUDETS OPPGAVER

- Være kontaktpunktet for de registrerte (de som har gitt personopplysninger til organisasjonen).
- Informere og gi råd til organisasjonen og de ansatte og frivillige.
- Bidra til at regelverket til fulgt.
- Gi råd om og delta i arbeidet med konsekvensanalyser.
- Fungere som kontaktpunkt mellom Datatilsynet og organisasjonen.

Politiattest, ekskludering og personvern

POLITIATTEST

Det er vanlig at barne-og ungdomsorganisasjoner innhenter politiattest for personer som har et tillits- eller ansvarsforhold for mindreårige i organisasjonen.

Politiattesten skal legges fram for den som er utnevnt som ansvarlig for politiattester og eventuelt denne personens vara. Disse har taushetsplikt og kan ikke dele informasjon om innholdet av attesten med andre.

En politiattest som er vist fram og uten anmerkninger registreres i en database med dato for når attesten ble vist fram og med informasjon om til hvem. Attesten beholdes av den det gjelder.

Dersom det er anmerkninger knyttet til attesten eller om attesten ikke blir fremvist, er det ikke anledning til å la vedkommende utføre oppgaver i organisasjonen.

En politiattest med anmerkning inneholder sensitive opplysninger. Informasjonen som fremgår av politiattesten skal behandles helt konfidensielt. Det er kun politiattestansvarlig/vara og eventuelt styrets leder som skal kjenne til innholdet i politiattesten. De har alle taushetsplikt om opplysninger knyttet til politiattesten.

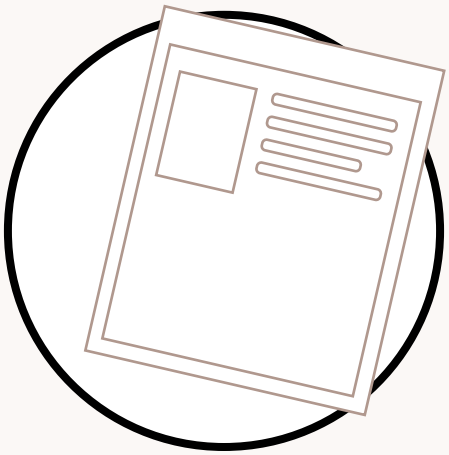
EKSKLUDERING AV PERSONER I ORGANISASJONEN

Enkelte ganger opplever organisasjoner saker hvor frivillige personer blir ekskludert på grunn av grenseoverskridende atferd. Informasjon om slike saker er sensitiv, men samtidig viktig for organisasjonen. Organisasjonen må sikre at personen det gjelder ikke utgjør en risiko for organisasjonens omdømme eller tillit fra medlemmer og samarbeidspartnere.

I slike tilfeller er det viktig å begrense tilgangen til informasjonen om saken og personen det gjelder, men samtidig gjøre den tilgjengelig for nøkkelpersoner. Informasjonen kan sikres med rolletilgang og god informasjonssikkerhet.

LAGRINGEN AV INFORMASJONEN MÅ SKJE PÅ BAKGRUNN AV EN RISIKOVURDERING

- Hvem må kjenne til informasjonen om vedkommende?
- Hvor mye informasjon trenger dere å oppbevare for å sikre organisasjonens?
- Det må også gjøres en vurdering av hvor lenge informasjonen må oppbevares.
- Dokumenter rutinene dere har ved ekskludering av personer i organisasjonen.



Årshjul for å sikre et godt personvern i organisasjonen

Ledelsen er ansvarlig for at det settes av nok ressurser til å ivareta internkontroll og sørge for tilstrekkelig informasjonssikkerhet i organisasjonen.

INFORMASJONSSIKKERHET

Ta en full gjennomgang av rutiner rundt informasjons-sikkerhet. Kjør en risiko/sårbarhetsanalyse rundt de enkelte persondataene. Har dere gode og sikre passord? Adgangskontroll -hvem må ha tilgang til hva? Hvordan sikre alle persondata, både de som er lagret elektronisk og fysisk.

ENDRINGER I REGELVERKET

For en eventuell revidering av interne rutiner og dokumenter, er det lurt å oppdatere seg om det har skjedd endringer i regelverket siden sist.

GJENNOMGANG AV AVVIK

Organisasjonen går gjennom hendelser og avvik som har skjedd det siste året. Det bør ses spesielt på årsaker for avviket og hvordan avvik og hendelser er håndtert.

OPPDATERE DOKUMENTASJON

Følgende materiell og dokumentasjon bør gjennomgå en årlig revidering: Personvernerklæring, skjemaer for samtykke, intern dokumentasjon for håndtering av alle persondata, avvikshåndtering + andre rutiner knyttet til persondata.

EGENKONTROLL OG OPPFØLGING

Skriv referat fra gjennomgangen og lag en plan for oppfølging og egenkontroll av det som kom fram.

Når har dere lov til å behandle personopplysninger?

Det er visse kriterier som må ligge til grunn for at man skal ha lov til å samle inn og bruke personopplysninger. Dette omtales ofte som behandlingsgrunnlag.

HAR VI LOV?

Foreligger det et samtykke? Eller foreligger det en lovhjemmel? Er behandlingen av persondataene nødvendig for å oppfylle en avtale?

GIR DERE TILSTREKKELIG INFORMASJON?

Det må gis tilstrekkelig med informasjon om hva som skal gjøres med personopplysningene til den det angår. Dette gjøres i en personvernerklæring, og i det skriftlige materiellet som gis ved et samtykke. I den nye forordningen er det økt krav til at informasjonen skal være forståelig for mottakeren. Husk at informasjon til barn skal tilpasses barnets forståelsesnivå.

HVA BRUKES OPPLYSNINGEN TIL?

Formålet med innhenting og bruk av personopplysningene må være tydelig og enkelt formulert fra organisasjonen. Det vil si at det ikke er rom for å bruke vage eller vide begrunnelser og bruken må være relevant for formålet. Persondataene må dekke et behov hos organisasjonen og dataene kan ikke brukes til andre/nye formål.

HVA ER NØDVENDIG?

Dere skal ikke samle inn flere personopplysninger enn dere trenger for eksempelvis å kunne registrere et nytt medlem. Samtidig skal ikke persondataene oppbevares lengre enn nødvendig.

RIKTIGE OG SANNE OPPLYSNINGER?

Opplysningene dere har lagret om en person må være riktige og oppdaterte.

SIKKERHET FOR PERSONDATAENE

Personopplysningene må være sikret med tilstrekkelig informasjonssikkerhet hos ansatte og tillitsvalgte, gjennom gode passord, sikre datasystemer, konfidensialitet mm.