Personvernhandbok

for kommunane på

Søre Sunnmøre

Versjon 1.2 – 1.1.2020

1 Personvernhandbok for kommunane på Søre Sunnmøre «7-stjerna»

Kvifor er personvern så viktig?

Det er eit sterkt fokus i samfunnet på korleis våre personopplysningar vert nytta og lagra, og stigande forventningar til at verksemder og offentlege myndigheiter tek dette på alvor.

Personvern har sitt utspring i at alle menneske har ein ukrenkeleg eigenverdi. Som enkeltmenneske har du derfor rett på ei privat sfære som du sjølv kan kontrollere, her kan ein handle fritt utan tvang eller innblanding frå staten eller andre menneske. Personvern er ikkje berre ein viktig menneskerett som skal sikre omsynet til den enkelte sin personlege integritet og privatliv. Personvern er også viktig for å sikre felles gode i eit demokratisk samfunn. Utan rett til å ha eit privatliv vil det ikkje vere mogleg for det enkelte menneske å skape seg eit rom til å utvikle refleksjonar og vurderingar på eit sjølvstendig grunnlag, utan å bli forstyrra eller kontrollert av andre.

Som ein del av dette er enkeltpersonar sin rett til å ha innflytelse på bruk og spreiing av personopplysningar om seg sjølv. Vi skal i størst mogleg grad kunne bestemme over eigne personopplysningar. Med dei nye personvernreglane som er innført i heile EU/EØS frå 2018, har desse rettigheitene blitt ytterligare styrka. Innbyggjarane har fått nye rettigheiter knytt til bruk av personopplysningar, dei skal ha meir opplysningar/informasjon om bruken av personopplysningar og ein må oftare enn før vurdere personvernet ved nye tiltak eller når ein tek i bruk nye dataprogram.

Datatilsynet er gitt mynde til å i legge bøter for brot på regelverket knytt til personvern. Rutinane er ein del av internkontrollen til kommunane og er viktig dokumentasjon på at vi arbeider for eit godt personvern for innbyggjarane. Her vil vi understreke at det er svært viktig at rutinane vert tatt i bruk og at det er eit leiaransvar å inkorporere personvern i det daglege arbeidet i kvar sektor/avdeling.

I personvernhandboka finn du først ei forklaring på dei mest sentrale omgrepa knytt til personvern, vidare kjem blant anna rutinar både for rettigheitene til innbyggjarane, opplysningsplikta som kommunen har og rutine for når og korleis ein skal vurdere personvernet (DPIA). Du finn også rutinar for kva ein gjer med ustrukturerte data, altså personopplysningar som ikkje ligg i dei sak/arkivsystem kommunane skal nytte, rutine for når ein skal melde frå til Datatilsynet ved avvik, og rutine for bruk av bilete i kommunane sin regi. På dei siste sidene i personvernhandboka finn du malar som vi håper vil gjere det enklare å inkorporere dei nye reglane for personvern i ditt arbeidsområde.

Denne personvernhandboka er utarbeidd av ei interkommunal arbeidsgruppe i sjustjerna, og det er personvernomboda som er ansvarlege for å oppdatere handboka.

Dersom du har spørsmål, merknader eller kommentarar til rutinane er det berre å ta kontakt med personvernombodet i di kommune.

Innhald

2 Generelt

2.1 Avklaring av omgrep

Under finn du definisjonar på enkelte omgrep som vert nytta i denne handboka. For ei meir utfyllande oversikt, sjå Datatilsynet si ordliste.

Behandlings-ansvarleg	Den som fastset formålet med behandlinga av personopplysningar og kva hjelpemiddel som kan nyttast. Dette vil vere kommunen.
Behandling av personopplysningar	Alt ein gjer med personopplysningane som t.d. innsamling, registrering, organisering, strukturering, lagring, tilpassing eller endring, attfinning, konsultering, bruk, utlevering ved overføring, spreiing eller alle andre former for tilgjengeleggjering, samanstilling eller samkøyring, avgrensing, sletting eller destruksjon.
Databehandlar	Ein fysisk eller juridisk person, ein institusjon, offentleg myndigheit eller eit anna organ som behandlar personopplysningar på vegne av den behandlingsansvarlege (oftast ein leverandør av IT-tenester).
Dataportabilitet	Betyr at ● den enkelte har rett til å få utlevert personopplysningane sine og til å lagre dei på ei privat eining til vidare og personleg bruk ● den enkelte har rett til å flytte, kopiere eller overføre personopplysningane sine fra ei verksemd til ei anna
Den registrerte	Ein fysisk person som personopplysingane kan knytast til. Dette kan til dømes vere ein pasient, brukar, elev, føresett eller tilsett.
Integritet	At personopplysningar ikkje vert endra ved behandling, anten utilsikta eller uautorisert.
Konfidensialitet	At sensitive personopplysningar ikkje blir kjent for uvedkomande, dvs. at berre autorisert personell skal ha tilgang til slike opplysningar; og slik tilgang skal kunne sporast/kontrollerast.
Personopplysningar	Ei opplysning eller vurdering som kan knytast til oss som enkeltpersonar, slik som for eksempel namn, adresse, fødselsdato, personnummer, telefonnummer, e-postadresse, IP-adresse, bilnummer, bilete, fingeravtrykk. Opplysningar om åtferdsmønster er også rekna som personopplysningar. Opplysningar om kva du handlar, kva butikkar du går i, kva tv-seriar du ser på, kvar du beveger deg i løpet av ein dag og kva du søker etter på nettet er alt saman personopplysningar. Det same gjeld opplysningar innhenta ved kameraovervaking og adgangskontroll med t.d. nøkkelkort.
Personvernombod	Eit personvernombod er ei lovpålagt rolle som alle kommune må ha i medhald av det nye regelverket.
Profilering	Analysering av personopplysningar for å avdekke åtferd, evner, preferansar eller

	behov
Sensitive opplysningar	Dette er til dømes opplysningar om rasemessig eller etnisk bakgrunn, eller politisk, filosofisk eller religiøs oppfatning, at ein person har vore mistenkt, sikta, tiltalt eller dømd for ei straffbar handling, helseforhold, seksuelle forhold eller medlemskap i fagforeiningar.
Tilgjengelegheit	At personopplysningar/ informasjonen til ei kvar tid er tilgjengeleg for dei som skal behandle den.
Tredjepart	Ein kvar annan fysisk eller juridisk person, offentleg myndigheit, institusjon eller eitkvart anna organ enn den registrerte, den behandlingsansvarlige, databehandlaren og dei personar som under den behandlingsansvarlege eller databehandlarens direkte mynde har fullmakt til å behandle personopplysningar.
Ustrukturerte data/ personopplysningar	Dette er data vi har samla som ikkje er søkbare (er i eit arkivsystem). Døme kan vere rekneark, word-dokument, diverse e-postar, papir vi har i permar på kontoret, data vi har sendt overført til private PC-ar, lydfiler, bilete av elevar på telefonen eller minnepenn etc.

2.2 Kontroll av identitet

Det er viktig at ein kontrollerer at personar som kontaktar kommunen om til dømes innsyn, korrigering og sletting faktisk er den registrerte. Dette for å sikre at vi mellom anna overheld teieplikta vår, og ikkje gjev uvedkomande personar innsyn i ein registrert sine opplysningar.

Korleis sikre identitet?

Vi kan krevje å få framvist legitimasjon (pass, førarkort, bankkort eller anna ID).
Dette er i utgangspunktet ikkje naudsynt dersom:

- Kommunikasjonen er via Digital Post / eDialog (sikker kanal)
- Namn og adresse er identisk med dei opplysningane som elles går fram av saka. Dette fordi opplysningane vil verte sendt til den registrerte på denne adressa.

NB! Det er til dømes ikkje tilstrekkeleg identifikasjon av den registrerte, at vedkomande på telefon eller ved personleg oppmøte, opplyser om eit personnummer. I slike tilfelle må det stillast kontrollspørsmål som gjer at du kan bekrefte identiteten til vedkomande.

Dersom ein registrert er representert av andre, må vi også sikre at denne representanten har mynde (fullmakt) til å handle på vegne av den registrerte. Dersom representanten er ein advokat eller revisor, vil det som utgangspunkt ikkje vere naudsynt å krevje fullmakt, med mindre saka sin karakter eller omstenda tilseier det.

Dersom kommunen får e-post frå ein person, og vi ikkje direkte kan identifisere avsendaren, må vi be om ytterlegare identitetsopplysningar.

Dersom det ikkje er mogleg for kommunen å identifisere den registrerte, skal vi, så langt det er mogleg, informere den registrerte om det.

I tilfelle der vi ikkje kan identifisere den registrerte, skal ikkje kommunen overhalde den registrerte sine rettar om innsyn, sletting, avgrensa behandling, underretning av tredjepart og dataportabilitet.

2.3 Utsending av informasjon

All korrespondanse og informasjon skal sendast elektronisk, dersom det er mest hensiktsmessig. NB! Sensitive personopplysingar, sjå definisjon under punktet «generelt», skal ikkje sendast på e-post, heller ikkje opplysingar som ved å kome på avvegar lett kan misbrukast, typisk fødsels- og personnummer.

Det er ikkje krav om at kommunen gir informasjonen i et bestemt format. Det er eit krav at informasjonen vert formidla på ein klår, konsis og lettforståeleg måte.
Merk at informasjon til born og personar med særskilde utfordringar må tilpassast slik at desse får tilstrekkeleg oversikt over kva saka gjeld.

2.4 Risikovurderingar

Når eit system som behandlar personopplysningar skal kjøpast inn, endrast eller utviklast må det gjerast ei risikovurdering. Vurderinga skal sikre at opplysningane vert behandla i samsvar med lovkrav. Kravet om å gjere ei risikovurdering følgjer (implisitt) av personvernforordninga artikkel 5 og artikkel 24 samt artikkel 32. Eit utgangspunkt for risikovurderinga vil vere ei ROS-analyse (risiko og sårbarheitsanalyse). Risikovurderinga etter GDPR skal ha fokus på risiko for den registrerte.

Målet med risikovurderinga er å kartleggje om det må setjast i verk sikringstiltak. I tillegg vil risikoanalysa vere viktig dokumentasjon ved til dømes eit personvernbrot og dokumentasjon på at ein overheld krava i personvernforordninga. Resultatet frå risikovurderinga vil avgjere om det er nødvendig med ei personvernkonsekvens-utgreiing, jf. punkt 11 «Vurdering av personvernkosekvens - DPIA».

I ei kartlegging av risiko er det særleg relevant å vurdere risikoen for utilsikta eller ulovleg tilintetgjering, tap, endring eller ikkje-autorisert utlevering av, eller tilgang til opplysningane, samt kva tiltak som må settast i verk å hindre dette. Høgre risiko krev fleire/meir omfattande tiltak.

Ved behandling av personopplysningar må følgande dokumenterast

- At det er gjort ei risikoanalyse over behandlinga, som viser sannsyn for og konsekvens av risiko
- Kva tiltak som er gjorde for å hindre eller redusere risiko.

3 Rettsleg grunnlag for behandling av personopplysningar

«Lov om behandling av personopplysningar (personopplysningsloven) § 1 og forordning (EU) 2016/679 om personvern Art. 6, 9 og 10»

Den nye personopplysningslova krev at vi må ha ein heimel for å kunne behandle personopplysningar. Vidare er det forbode å behandle særskilde kategoriar av personopplysningar (sensitive opplysningar) utan rettsleg grunnlag.

Det er seks moglege grunnlag for å kunne behandle personopplysningar. Desse går fram av art. 6 i forordninga. Artikkel 9 og 10 fastset ytterlegare reglar om behandling av særskilde kategoriar av personopplysningar, og om straffedommar og lovbrot.

Det er viktig at du tek stilling til om du har heimel, før du tek til å behandle personopplysningar, og du må dokumentere skriftleg at du har eit rettsleg grunnlag.

Det vil vere eit brot på regelverket om du ikkje på ein klår og tydeleg måte har identifisert kva rettsleg grunnlag du nyttar for behandlinga.

Du kan ikkje skifte til eit anna rettsleg grunnlag for å oppnå det same formålet med behandlinga, med mindre du har ein god grunn til det.

Ver merksam på at dersom behandlingsgrunnlaget er samtykke eller berettiga interesse, gjeld det eigne krav til dokumentasjon.

Konsekvensen av å ikkje ha lovleg heimel, er at behandlinga av personopplysningar er ulovleg, og må opphøyra straks.

Personvernforordninga gjeld ikkje for aktivitetar knytt til strafferetts. Det inneber at kommunen lovleg kan gje opplysningar i samband med etterforsking, førebygging, og straffeforfølging. Kommunen kan til dømes utlevere dokument på førespurnad frå politiet, utan omsyn til GDPR. Slike forhold vert regulert i særlover.

3.1 Oversikt over lovleg heimel for behandling av personopplysningar

Samtykke frå den registrerte
Samtykke frå den registrerte – vedkomande har gjeve eit klart og frivillig samtykke til at kommunen kan behandle vedkomande sine personopplysningar.

NB! Det gjeld strenge krav for når eit samtykke er gyldig.
Sjå eiga rettleiing for samtykke.

Når det gjeld samtykke må du kunne dokumentere følgande:

- At vi har motteke samtykke
- Kva samtykket spesifikt gjeld
- Kven som har gjeve samtykke
- Korleis samtykke vart gjeve
- Når samtykke vart gjeve
- Kva informasjon den registrerte fekk **før** han/ ho ga sitt samtykke.

Naudsynt for å oppfylle avtale
Det er naudsynt å behandle personopplysningar for å oppfylle avtale som den registrerte er part i, eller gjennomføre tiltak på den registrerte sin førespurnad før avtaleinngåing.
Dette kan for eksempel vere ein arbeidsavtale.

Plikter kan også følge meir implisitt, for eksempel om utbetaling av løn til bankkontoen til ein tilsett, utan at kontonummeret står i arbeidsavtalen.

Merk at ein avtale kan aldri vere behandlingsgrunnlag for sensitive personopplysingar.
Det er ikkje naudsynt at den aktuelle avtalen er skriftlig. Den kan være munnleg eller inngått digitalt, men du må dokumentere at ein slik avtale er inngått, når og kva den går ut på m.m.

Naudsynt for å oppfylle ei rettsleg plikt
Ein har rettsleg grunnlag til å behandle personopplysningar dersom dette er naudsynt for å oppfylle ei rettsleg plikt som kvilar på kommunen (ikkje kontraktshøve). Dette er i dei tilfella der kommunen er må behandle personopplysningar for å kunne etterleve lovverket.
Døme:
Bokføringslova, som pålegg verksemda å oppbevare rekneskapsmateriale, som kan innehalde personopplysningar

A-opplysningslova, som pålegg alle arbeidsgjevarar å sende opplysningar om tilsetjingshøve til Skatteetaten, NAV og Statistisk sentralbyrå kva månad.

Naudsynt for å verne om den registrerte
Vi kan behandle personopplysningar dersom dette er naudsynt for å verne om den registrerte eller ein annan person sine vitale interesser – som til dømes å redde nokon sitt liv.

Naudsynt for å utføre ei oppgåve i ålmenta si interesse eller utøve offentleg mynde
Dette er i dei tilfella der det er naudsynt å utføre ei oppgåve i ålmenta si interesse eller utøve offentleg mynde (den siste er den viktigaste for kommunen) – til dømes tildeling av sjukeheimsplass. Ein føresetnad for å nytte dette grunnlaget er at det ligg føre ei lov eller ei forskrift, som pålegg kommunen oppgåver som gjer det nødvendig å behandle personopplysningar.

Det er ikkje eit krav at lova seier noko konkret om behandling av personopplysningar, men det må vere nødvendig å behandle opplysningane for å kunne utføre det lova krev. Den aktuelle lova eller forskrifta må identifiserast, det er ikkje nok å seie at behandlinga er «nødvendig for å utøve offentleg mynde» utan å vise til ein ytterligare heimel.

Merk at det gjeld strengare krav dersom utøvinga av offentleg mynde inneber behandling av sensitive personopplysningar, sjå punkt 3.5 (under).

Offentleg myndigheit og teiepliktige opplysningar

I nokre tilfelle kan det vere nødvendig å innhente/dele teiepliktige opplysningar frå andre organ, til dømes frå folkeregisteret eller politiet. For å innhente/ dele slike opplysningar må det anten innhentast samtykke frå den registrerte, eller så må ein ha ein lovheimel som seier noko konkret om det å hente inn og dele personopplysningar.

Eit døme på dette er barnehagelova § 22 a som seier at «offentlige myndigheter kan uten hinder av taushetsplikt innhente opplysninger fra Folkeregisteret…».

Naudsynt for formål knytt til ei berettiga interesse
Dette grunnlaget skal nyttast når det er nødvendig å behandle personopplysningar for formål knytt til ei berettiga interesse, med mindre den registrerte sine interesser og fridom går framfor(interesseavveging)».

NB! dette grunnlaget kan ikkje nyttast av kommunen når vi behandlar personopplysningar for å utøve offentleg mynde.

Å nytte berettiga interesse som rettsleg grunnlag kan vere aktuelt ved til dømes videoovervaking av kommunal grunn/ eigedom, sikringstiltak som adgangskontroll eller når kommunen er arbeidsgjevar.

Det må ligge føre ei interesse som gjer det nødvendig å behandle personopplysningar. Det er kommunen som må skildre og dokumentere kva den konkrete berettiga interessa er.

Det inneber at du må ta stilling til følgande:

- kvifor du ønsker å behandle opplysningane
- kor viktig er det å behandle opplysningane?
- kva skjer om du ikkje gjer det?
- er behandlinga uetisk på nokon måte?

Vidare må behandlinga vere naudsynt for å oppfylle den berettiga interessa. Det vil seie at det må vere ein samanheng mellom behandlinga og interessa. Samanhengen treng ikkje vere kritisk eller tvingande nødvendig for verksemda, men kan ikkje vere for fjern eller hypotetisk.

Vi må alltid vurdere om det er andre måtar ein kan oppnå det ønska resultatet på? Om svaret på dette spørsmålet er nei, vil behandlinga fort verte vurdert som «naudsynt».

Dersom utfallet av vurderinga er at det ligg føre ei berettiga interesse, og behandlinga av personopplysningar er naudsynt for å oppnå denne interessa, må det gjerast ei interesseavveging.

Utgangspunktet for avveginga er på den eine sida kommunen sitt behov, og på den andre sida den registrerte sitt behov.

Ein grunnleggande test kan være å spørje seg sjølv om den registrerte vil verte negativt overraska når vi informerer dei om korleis vi behandlar deira personopplysningar. Dersom svaret er ja, kan det vere at eit samtykke er eit meir passande grunnlag for behandlinga.

3.2 Hjelpespørsmål i interesseavveginga

Avveginga vert ikkje avgjord ved å telle talet på ja og nei. Du må vurdere alle faktorane og vege dei i mot kvarandre.

• Har den registrerte bedt om at registreringa skal skje? • Reknar den registrerte med at behandlinga finn stad? • Vil den registrerte ha fordelar av behandlinga, som til dømes betre tenester? • Er behandlinga i den registrerte si interesse? • Har kommunen og den registrerte same interesse? • Er det eit gjensidig forhold mellom kommunen og den registrerte? • Er det få opplysningar om den registrerte som vil bli behandla? • Er det snakk om faktiske opplysningar? • Har den registrerte gitt opplysningane sjølv? • Er kommunen komfortabel med å gi den registrerte god informasjon om behandlinga? • Gir kommunen god informasjon om behandlinga til den registrerte? • Er det enkelt for den registrerte å kontakte kommunen for å kontrollere behandlinga?	Viss JA - interessa er i kommunen sin favør og vi kan samle inn personopplysningane.
• Vil den registrerte bli overraska over behandlinga? • Vil den registrerte kunne oppfatte behandlinga som negativ? • Kan den registrerte oppfatte behandlinga som irriterande eller upassande - med tanke på forholdet mellom skulen og den registrerte? • Innheld opplysningane vurderingar av den registrerte? • Vil det bli behandla mange opplysningar om den registrerte? • Er det snakk om uvanleg behandling av opplysningar? • Er det mogleg for kommunen med ei mindre inngripande behandling av opplysningane?	Viss JA talar det imot at kommunen skal behandle person-opplysningane.

3.3 Kva behandlingsgrunnlag skal nyttast?

Som utgangspunkt skal kvart formål berre ha eit behandlingsgrunnlag. Dersom du har fleire behandlingsgrunnlag som kan nyttast for same formål/aktivitet, skal berre eitt grunnlag veljast. I nokre tilfelle er det nødvendig å nytte fleire grunnlag. Dersom ei lov ikkje gjev heimel til alle dei nødvendige behandlingane, vil det i tillegg vere naudsynt å til dømes innhente eit samtykke, eller nytte berettiga interesse som behandlingsgrunnlag.

Eit døme på dette er tildeling av kommunal bustad for «vansklegstilte». Etter sosialtenestelova pliktar kommunen å medverke til å skaffe bustadar. For å kunne tilby bustader det nødvendig for kommunen å behandle personopplysningar som namn, kontaktinformasjon, identitet o.l. For å kunne prioritere kven som skal få bustad vil det kunne vere nødvendig å innhente til dømes helseopplysningar, rushistorikkeller andre personlige forhold. Ettersom lova ikkje gjev heimel for å innhente til dømes helseopplysningar, må den registrerte samtykke til at slike opplysningar vert innhenta, delt med andre etatar med meir.

For skule- og barnehagesektoren har Utdanningsdirektoratet utarbeidd ei rettleiing. Sjå også Datatilsynet sine heimesider.

3.4 Kva skjer om vi har eit nytt formål?

Dersom formålet ditt endrar seg over tid, og du har eit nytt formål som du ikkje var klar over i starten, så treng du ikkje eit nytt grunnlag, så lenge det nye formålet samsvarar med det opphavelege. Merk at dette ikkje gjeld om den opphavelege heimelen for behandling av personopplysningar er basert på eit samtykke. Då må du anten innhente eit nytt samtykke, eller eit nytt rettsleg grunnlag for behandlinga.

Artikkel 6 nr. 4 i forordninga inneheld ei ikkje-uttømmande liste av moment som vi må vurdere i høve spørsmålet om et nye formålet samsvarar med det opphavelege innsamlingsformålet:

- Det skal takast omsyn til ein kvar samanheng mellom dei formåla som personopplysningane er samla inn for, og formåla med den tiltenkte vidarebehandlinga
- I kva samanheng er personopplysningane samla inn. Særleg med omsyn til forholdet mellom den registrerte og kommunen
- Arten av personopplysningane som behandlast, særleg om dette er sensitive opplysningar
- Moglege konsekvensar av den påtenkte vidarebehandlinga for den registrerte

Dersom det nye formålet ikkje samsvarar med innsamlingsformålet, må vidarebehandlinga ha grunnlag anten i lov eller samtykke. At denne behandlinga må ha grunnlag i lov eller samtykke, inneber at lovgrunnlaget eller samtykket må knytte seg til sjølve vidarebehandlinga for ikkje-samsvarande føremål.

3.5 Nærare om særlige kategoriar av personopplysningar(sensitive personopplysninger)

Særlege kategoriar av personopplysningar/sensitive personopplysningar er omtala i personvernforordninga artikkel 9 .

Det er strengare krav til behandling av sensitive opplysningar/særlege kategoriar av personopplysningar. Utgangspunktet er at slik behandling er forbode. Det må difor undersøkast om ein har eit lovleg behandlingsgrunnlag for å behandle opplysningane I tillegg til at ein må ha behandlingsgrunnlag etter artikkel 6 (sjå punkt 3 over). Det må dokumenterast både kva behandlingsgrunnlag etter i artikkel 6 og kva føresegn i artikkel 9 som er nytta.

Kva skal reknast som særlege kategoriar av personopplysningar (sensitive personopplysningar)?

Dette er til dømes opplysningar om rase eller etnisk bakgrunn, eller politisk, filosofisk eller religiøs overbevising, at ein person har vore mistenkt, sikta, tiltalt eller dømd for ei straffbar handling, helseforhold, seksuelle forhold eller medlemskap i fagforeiningar.

Merk at terskelen for å seie at noko skal reknast som eit helseforhold er låg. Det kan til dømes opplysningar om helsetilstand, allergiar, sjukefråvær, graviditet eller legebesøk.

Når kan sensitive opplysningar behandlast?

For det første må kommunen ha eit gyldig behandlingsgrunnlag, sjå punkt 3.1. I tillegg må eit av unntaka i artikkel 9 nr. 2 vere oppfylt.

Dei mest aktuelle unntaka for kommunen i artikkel 9 nr.2 for å behandle sensitive personopplysningar er:

- Uttrykkeleg samtykke til å behandle dei sensitive opplysningane.
- Nødvendig for å oppfylle forpliktelsar/rettar innan arbeidsretten, trygderetten og sosialretten. I tillegg må ein ha lov- eller forskriftsheimel. (f.eks. folketrygdloven).
- Nødvendig for å verne vitale interesser, når den registrerte ikkje er samtykkekompetent (til dømes for å redde liv).
- Nødvendig for å fastsetje, gjere gjeldande eller forsvare eit rettskrav. (til dømes om kommunen blir saksøkt)
- Nødvendig for yting av helsetenester. I tillegg må kommunen ha heimel i lov, og den som gjer behandlinga må være pålagd teiepliktplikt i lov. (til dømes pasientjournalloven)
- Nødvendig for allmenne folkehelseomsyn. Det er i tillegg krav om lovheimel (til dømes helseregisterloven.)
- Nødvendig for arkivformål i ålmenta si interesse. I tillegg kravst det heimel i lov (til dømes arkivlova og arkivforskrifta).

Merk at det er strengare krav til presis lovheimel når ein behandlar særlege kategoriar av personopplysningar enn «vanlege» opplysningar. Lova må seie konkret kva behandlingar som er lov, som til dømes kva opplysningar som kan samlast inn, kven opplysningane kan delast med, lagringstid eller liknande.

3.6 Sjekkliste- behandlingsgrunnlag

Krav	**Ja/ Nei**
Vi har vurdert formålet med behandlinga av personopplysningar, og valt det mest passande behandlingsgrunnlaget for kvar aktivitet.	
Vi har vurdert at behandlinga er nødvendig for det relevante formålet, og er overtydd om at det ikkje er mogleg å oppnå formålet på ein annan måte.	
Vi har dokumentert skriftleg kva rettsleg formål vi nyttar, og at vi fyller regelverket.	
Vi har inkludert informasjon både om formålet med behandlinga og behandlingsgrunnlaget i vår personvernerklæring.	
Når vi behandlar sensitive personopplysningar har vi også identifisert vilkåra for at vi kan behandle desse, og dokumentert dette.	
Når vi behandlar opplysningar om straffedommar, tiltale med meir, har vi også identifisert grunnlaget og vilkåra for å behandle desse, og dokumentert dette.	

3.7 Særskilt om samtykke

Samtykke som rettsleg grunnlag for behandling av personopplysningar er omtala i *personvernsforordninga art. 4 (11), 6 (1 a) 7 og 9 (2 a)*

Formålet med denne rettleiinga er å forklare:

1. Når eit samtykke er gyldig
2. Kva det inneber juridisk at eit samtykke vert trekt attende.

Rettleiinga inneheld også ei sjekkliste du kan nytte som ei retningslinje for om samtykket oppfyller lova.

Etter personopplysningslova og personvernforordninga kan ikkje kommunen innhente personopplysningar utan at det ligg føre eit konkret formål og eit rettsleg grunnlag.

Eit samtykke frå personen vi ønsker å innhente personopplysningar av er eit av fleire rettslege grunnlag for behandling av personopplysningar.

Du må alltid vurdere om det ligg føre andre rettsgrunnlag som kan vere betre eigna enn samtykke (t.d. berettiga interesse). Dette fordi ein registrert kan trekkje tilbake eit samtykke når han/ho måtte ønske det.
Som hovudregel vil lovheimel vere det rettsgrunnlaget kommunen nyttar.

Kva er eit samtykke?
Det går fram av personvernforordninga art. 4 nr. 11 at eit samtykke er:

> «enhver frivillig, spesifikk, informert og utvetydig viljesytring fra den registrerte der vedkommende ved en erklæring eller en tydelig bekreftelse gir sitt samtykke til behandling av personopplysninger som gjelder vedkommende,»

Dette er eit uttrykk for at den registrerte skal ha ei reelt val om dei vil gje frå seg personopplysningar, og kontroll over korleis deira personopplysningar vert nytta.

Nærare om krava til eit samtykke
Det er eit krav etter det nye regelverket at kommunen, der det ikkje føreligg anna rettsgrunnlag som t. d lovheimel, må dokumentere/ bevise at den registrerte har gjeve eit gyldig samtykke til at vi kan behandle vedkomande sine personopplysningar.

Det må mellom anna gå fram av dokumentasjonen:

- Kven som har gjeve samtykke
- Dato
- Kva det konkret er gjeve samtykke til

Det er viktig å merke seg at eit samtykke gjeld berre for det formålet vi har informert vedkomande om at det skal gjelde for.

Kvar eining må ha ei rutine for når det skal innhentast nytt samtykke, og kor lenge samtykket skal gjelde (t. d 1, 3 eller 5 år).

Dersom den registrerte sitt samtykke er gjeve i eit dokument, som også omhandlar andre høve, så skal samtykkeerklæringa skiljast ut i eige skjema. Samtykkeerklæringa skal vere i eit klårt og tydeleg språk.

NB! Det er viktig at vi opplyser vedkomande, før samtykket vert gjeve, om at eit samtykke kan trekkast tilbake når som helst. Dersom dette ikkje er gjort, vil samtykket som hovudregel verte rekna som ugyldig.

Oppfyller ikkje samtykket krava i regelverket, kan det ikkje nyttast som lovleg grunnlag for behandling av personopplysningar.

Tidspunkt for når vi må ha samtykket
Eit samtykke må vere innhenta før vi byrjar å behandle dei personopplysningane som samtykket gjeld.

Formkrav
Eit samtykke kan vere munnleg, skriftleg og digitalt.

Det avgjerande er at den registrerte si erklæring eller handling tydeleg får fram den registrerte si hensikt og vilje.

Merk! Ferdigutfylte boksar, eit stillteiande eller underforstått samtykke oppfyller ikkje krava til eit gyldig samtykke. Ein må aktivt gjere vala sjølv.

Vi må som nemnt ovanfor dokumentere at den registrerte:

- Har gjeve eit samtykke til behandling av vedkomande sine personopplysningar
- Kva det spesifikt er gjeve samtykke til (innhaldet i samtykket) og når (dato)

Eit samtykke skal difor som hovudregel vere skriftleg, eller innhenta på ein annan måte som kan bevisast.

NB! Konsekvensen av at vi ikkje kan dokumentere at det ligg føre eit gyldig samtykke, er at eit samtykke vert vurdert å vere i strid med personvernregelverket. Vi har då ikkje lov til å behandle personopplysningane med heimel i dette rettsgrunnlaget.

Frivillig
Eit samtykke skal vere frivillig.

Formålet med eit samtykke er å gje den registrerte eit val og kontroll over deira personopplysningar. Dette inneber at eit samtykke ikkje kan gjevast under tvang, og at det ikkje er fordelar eller ulemper knytt til samtykket.

Ulikt styrkeforhold mellom partane
Det er viktig å vere merksam på at eit samtykke som utgangspunkt ikkje er gjeve frivillig dersom det er ei klar skeivheit mellom den som samtykker og behandlingsansvarleg (kommunen).

Offentlege myndigheiter
Dette kan vere tilfelle der den registrerte søkjer om offentlege ytingar hjå kommunen, eller hjå andre offentlege myndigheiter. Ofte vil vedkomande ikkje ha andre alternativ enn å gje samtykke til behandlinga, om vedkomande ønsker tenesta. Vi bør difor vurdere andre rettsgrunnlag for vår behandling av personopplysningar(til dømes lov, avtale, berettiga interesse).
Som hovudregel vil lovheimel vere det rettsgrunnlaget kommunen nyttar.

Tilsetjingsforhold
I tilsetjingshøve vil det typisk vere ulikskap mellom arbeidsgjevar og ein tilsett. Arbeidsgjevar må difor som hovudregel ikkje nytte samtykke som rettsleg grunnlag. Om samtykke vert nytta må arbeidsgjevar vere merksam på korvidt den tilsette sitt samtykke er eit reelt uttrykk for den tilsette sitt val, eller om det er gjeve med frykt for negative konsekvensar. I sistnemnde tilfelle er ikkje samtykket gjeve frivillig. Ofte vil arbeidsavtalen eller berettiga interesse vere meir egna enn samtykke i eit tilsetjingsforhold

Samtykke som føresetnad for kontrakt
Vi skal aldri samle inn fleire personopplysningar enn det som er naudsynt.

Kommunen som behandlingsansvarleg må difor vere spesielt merksam på kva informasjon som er påkravd for å oppfylle ei kontrakt.

Spesifikt
At eit samtykke skal vere spesifikt betyr at det ikkje kan vere generelt utforma, eller utan ei presis skildring av kva formålet med behandlinga av personopplysningane er. Eit samtykke skal vere konkretisert på ein slik måte at det går klårt og tydeleg fram kva det er gjeve samtykke til. Dette inneber at personopplysningar berre skal vere innsamla til uttrykkeleg definerte og legitime formål (t.d. oppfylle kontrakt), og at dei ikkje kan behandlast på ein måte som er uforliklege med desse formåla.

Dersom behandlinga av personopplysningar skal tene fleire ulike formål, må vi innhente separat samtykke for kvart enkelt formål. I desse høva pliktar vi å legge til rette for at vedkomande får moglegheita til å samtykke til eit formål, og til å ikkje samtykke til andre. Dette kan praktisk løysast ved at vi utarbeider ei samla erklæring/ skjema der den registrerte kan krysse av, eller markere på andre måtar kva formål vedkomande samtykker til.

Når vi ber om eit samtykke må dette gjerast i ei form som er lett å forstå og lett tilgjengeleg. Språket må vere klårt og enkelt. Dersom samtykket er retta mot eit born må språket tilpassast barnet sin alder og utvikling. Sjå eige avsnitt om born og samtykke under.

Informert
Eit samtykke skal vere informert. Det betyr at den registrerte skal vite konkret kva han/ho samtykker til. For å sikre at den registrerte kan gjere ei avgjerd på informert grunnlag, må vi syte for at vi gjev nok opplysningar, og at alt som det skal samtykkast til går klårt fram.

Informasjonen kan gjevast skriftleg, digitalt eller munnleg. Det er viktig at vi dokumenterer skriftleg at vi har oppfylt plikta til å gje informasjon (til kven, når, kva har vi informert om).

Ved innhenting av samtykke frå besøkande på våre heimesider, må vi ha ei innretting som sikrar at vi overheld krava til eit gyldig samtykke. Dette kan vi gjere ved å ha ein kort tekst der dei besøkande klikkar «ja» for å ha lest og akseptert for å få vidare tilgang.

Minimumskrav til vår informasjon:

- Kontaktinformasjon til den behandlingsansvarlege og personvernombodet
- Formålet med den planlagde behandlinga
- Kva opplysningar som skal behandlast
- Kva behandling som skal skje, derunder om personopplysningane skal vidareformidlast til andre som til dømes offentlege myndigheiter, bedrifter m. m
- At eit samtykke når som helst kan trekkast tilbake og korleis det kan gjerast
- Den registrerte sine rettar (innsyn, korrigering, sletting m. m)

<u>Merk! Dersom vi til dømes ønsker å nytte bilete, eller vi lagar ein opplæringsvideo med nokon, kan det vere at det vil vere umogeleg å slette vedkomande i ettertid. Det må difor informerast spesifikt om at det ikkje vil vere mogleg å trekke tilbake eit samtykke i slike situasjonar.</u>

<u>Opplysningsplikt</u>
Når eit samtykke vert innhenta samtidig med at vi samlar inn personopplysningar frå den registrerte, vil vi i tillegg måtte oppfylle opplysningsplikta vår.
Sjå meir om opplysningsplikta i eigen rettleiar.

Tydeleg uttrykk for vilje
Den registrerte sitt samtykke skal vere tydeleg, og ein klar aksept av at vi kan behandle vedkomande sine personopplysningar. Det betyr at det ikkje må ligge føre omstende som gjev grunnlag for tvil om at samtykket er frivillig.

Ei slik erklæring kan til dømes vere i form av ei underskrift på eit dokument/ skjema, eller at det er kryssa av i eit felt på vår heimeside. Det kan vere tilstrekkeleg at den registrerte aksepterer ei erklæring om samtykke som er utfylt på førehand. Merk at sistnemnde krev at stadfestinga må gjerast ved ei aktiv handling frå den registrerte, som til dømes ved å klikke på eit felt som tydeleg opplyser den registrerte om at handlinga inneber eit samtykke til behandling.

Samtykke ved behandling av sensitive personopplysningar
Slike opplysningar har eit strengare vern etter regelverket, og det er forbode å behandle sensitive personopplysningar utan lovleg grunnlag. Dette inneber at det er særs viktig at det ikkje er nokon som helst tvil om at den registrerte sitt samtykke oppfyller krava i lovverket.

Passivitet
Tausheit-inaktivitet, felt på heimesider, eller skjema som er avkryssa på førehand, er ikkje eit samtykke, då dette ikkje er ei tydeleg viljesytring eller stadfesting.

Som tidlegare nemnt er det kommunen som skal dokumentere og bevise at det ligg føre eit uttrykkeleg samtykke. Det inneber at eit samtykke som hovudregel skal vere skriftleg.

Retten til å trekke attende eit samtykke
Det er viktig å vere merksam på at den registrerte fritt har rett til å trekkje attende sitt samtykket når som helst. Kommunen må difor gje informasjonen om at eit samtykke kan tilbakekallast, og måten dette kan skje på, samtidig med at vi innhentar samtykke frå vedkomande. Dersom dette ikkje er gjort, er ikkje samtykket gyldig.

Det er kommunen sitt ansvar å sikre at eit tilbakekall kan gjerast på ein enkel og lett tilgjengeleg måte. Det er ikkje eit krav at tilbakekallinga skal skje på same måten som samtykket vart gjeve.

Dersom samtykket er innhenta via ein nettstad, ein søknad, ein app, eller via e-post, bør den registrerte kunne trekkje tilbake sitt samtykke via same løysing. Det bør i tillegg vere fleire alternativ for tilbakekalling, ettersom ikkje alle har internett-tilgang eller er trygge brukarar av internett.

Eit tilbakekall skal kunne skje utan at det er til skade for vedkomande. Det inneber mellom anna at vi ikkje skal krevje gebyr, eller avgifter. Vi må opplyse den registrerte dersom konsekvensen blir at vi ikkje får behandla ein søknad, eit oppdrag eller liknande.

Kva med behandling som er gjort før tilbakekallinga av samtykket?
Eit tilbakekall av eit samtykke påverkar ikkje lovlegheita av ei behandling av personopplysningar som er gjort før tilbakekallet. Tilbakekallet får berre verknad for den framtidige behandlinga av personopplysningar.

Ved eit tilbakekall av eit samtykke er hovudregelen at vi må slutte å behandle informasjonen, så snart som mogleg. **NB! Oppbevaring av den registrerte sine opplysningar er også rekna som ei behandling og må difor må opphøyra**. Dette gjeld likevel berre for opplysningar som er innhenta på grunnlag av det tilbakekalla samtykket, og ikkje for opplysningar som er innhenta på eit anna rettsgrunnlag enn samtykke – til dømes ei kontrakt mellom kommunen og den registrerte, eller ein lovheimel.

Ved tilbakekall av samtykke har den registrerte som hovudregel rett til å få sine personopplysningar sletta. Sjå eiga rettleiing for sletting.

Sjølv om den registerte ikkje ber om det, må vi avgjere om informasjonen skal slettast der ei behandling er basert på eit samtykke, og det ikkje lenger ligg føre eit lovleg grunnlag i høve til oppbevaring av den registrerte sine opplysningar. I enkelte høve kan vi fortsetje behandlinga, om den er rimeleg i forhold til den registrerte (berettiga interesse). Merk at uvilje hjå den registrerte kan vere eit argument i mot at vi har berettiga interesse til å behandle personopplysningane.

Dersom vi har eit anna rettsleg grunnlag enn samtykke til å oppbevare opplysningane med eit anna sjølvstendig formål, som til dømes oppbevaring av opplysningar av omsyn til rekneskapslova og bokføringslova, vil behandlinga (oppbevaringa) kunne fortsetje.

Dersom behandlinga fortset på eit anna grunnlag, skal den registrerte ha informasjon om behandlingsgrunnlaget, formål m. m. Sjå eiga rettleiing om opplysningsplikt.

Born og samtykke

Born er særleg beskytta etter den nye personvernlova, då dei i mindre grad er klar over risikoen og konsekvensane som kan vere knytt til behandling av personopplysningar. Informasjonen, som vi pliktar å gje samstundes med innhentinga av samtykket, skal tilpassast barnet og vere på eit klårt og lett forståeleg språk.

Førebyggande eller rådgjevande tenester som vert tilbydd direkte til born, er ikkje omfatta av kravet. Born i alle aldrar skal kunne ta kontakt med offentlege eller private rådgjevarar utan samtykke frå føresette.

<u>Samtykke i skulen</u>

Formålet med eit samtykke er at den registrerte skal ha eit val og kontroll over eigne personopplysningar. Det betyr at det ikkje kan vere ujevnt styrkeforhold mellom partane. Dette kan vere tilfelle når ein lærar ber om samtykke frå ein elev, eller ein arbeidsgjevar ber om samtykke frå ein tilsett. I skulen bør vi derfor nytte lovheimel, og ikkje samtykke, som behandlingsgrunnlag.

Før skule - og barnehageeigar bruker samtykke som rettsleg grunnlag, anbefalar Utdanningsdirektoratet derfor at ein tek stilling til følgjande spørsmål:

- Kven har samtykkekompetanse? Barnet? Føresette? Barnevernet?
- Er samtykket reelt? Det vil seie at den som samtykker verkeleg har moglegheit til å seie nei til behandlinga (ein mister til dømes denne moglegheita om eit nei gjer at ein vert ekskludert frå viktige tenester).
- Har den som samtykker fått god nok informasjon om kva vedkomande samtykker til? Til dømes kva personopplysningane skal brukast til (formål). kven som er behandlingsansvarleg eller kor lenge personopplysningane skal lagrast.

Elevar kan sjølve gi samtykke frå dei er 15 år gamle. Før det må ein føresett samtykke. Unntak:

1. Sensitive personopplysningar skal berre innhentast med samtykke frå foreldra fram til barna har fylt 18 år.
2. For småkonkurransar og liknande, der enkle kontaktopplysningar berre skal brukast til eventuell premiering og deretter slettast, kan også mindre barn enn 15-åringar samtykke til deltaking sjølv. Her er det likevel ein føresetnad at opplysningane blir sletta etter premiering, at personverntrusselen er vurdert og klassifisert som særs låg, og at konkurransen er eigna for den aktuelle aldersgruppa.

3. Bruk av nettenester og appar slik som Facebook, Instagram og Snap, er særskilt regulert i personvernforordninga artikkel 8. I Noreg er aldersgrensa for å samtykke sjølv til bruk av denne typen tenester satt til 13 år.

Samtykket må vere henta inn før ein tek til å behandle dei opplysningane samtykket gjeld.

Kva med samtykke innhenta før den nye personvernlova vart sett i kraft?

Dersom vi behandlar personopplysningar på grunnlag av eit samtykke som vart innhenta før den nye lova vart sett i kraft, er det ikkje automatisk slik at vi må innhente eit nytt samtykke. Om samtykket vi allereie har innhenta er i samsvar med dei nye krava, vil det fortsatt vere gyldig.

Kvar eining i kommunen må gjennomgå sine rutinar og prosedyrar for samtykke, og vurdere om desse er i samsvar med det nye regelverket.

Det skal alltid innhentast nytt samtykke om eit samtykke ikkje er mogleg å tidfeste med dato.

3.8 Sjekkliste - Samtykke

Denne sjekklista kan tene som ei rettleiing for å sjå om kommunen si behandling er i samsvar med dei nye krava for samtykke. **Krav**	**Set kryss**
Vi har vurdert om eit samtykke er den mest føremålsmessige heimelen for vår behandling av personopplysningar for dette spesifikke formålet.	
Oppmodinga om samtykke er tydeleg og klart skilt frå anna tekst i dokumentet.	
Vi innhentar alltid samtykke gjennom eit aktivt val frå den samtykkande parten.	
Vi innhentar aldri samtykke via samtykkefelt som er førehandsutfylt, eller som på ein annan måte baserer seg på passivitet frå vedkomande.	
Samtykket er formulert på eit klart og enkelt språk som er lett å forstå for målgruppa og/eller aldersgruppa.	
Samtykket spesifiserer formålet med den påtenkte behandlinga av personopplysningane.	
Når vi ønskjer samtykke til fleire formål, spør vi om separate samtykke for kvart enkelt formål.	
Namnet på den behandlingsansvarlege og personvernombodet i kommunen går fram av samtykketeksten.	
Den registrerte har fått spesifikk informasjon om kor lenge samtykket gjeld.	
Vi har opplyst om at samtykket kan trekkjast tilbake når som helst, og korleis dette kan gjerast.	
Det er ikkje negative konsekvensar knytt til det å trekkje tilbake eit samtykke, i form av gebyr, avgifter og liknande.	
Dersom vi tilbyr onlinetenester direkte retta mot barn under 13 år, så nyttar vi berre samtykke dersom det er mogleg å sjekke barnet sin alder.	
Vi innhentar dei føresette sitt samtykke om barnet er under 13 år.	
Vi kan dokumentere skriftleg ● kven som har gitt samtykket ● når og korleis samtykket vart gitt ● kva den enkelte spesifikt har samtykka til ● at samtykket er reelt og gitt frivillig	
Vi følgjer regelmessig opp at samtykket er aktuelt og korrekt, og at formålet med behandlinga eller sjølve behandlinga ikkje har endra seg.	
Vi innhentar nytt samtykke om nødvendig.	

4 Rutine for opplysningsplikt

«Lov om behandling av personopplysningar» (personopplysningsloven) § 1 og personvernforordning art. 12, 13 og 14.

Denne rutinen skildrar korleis vi sikrar etterleving av plikta til å gje den registrerte opplysningar, når vi samlar inn personopplysningar om vedkomande.

Den saksbehandlar som samlar inn personopplysningar vil vere den som pliktar å gje opplysningar til den registrerte.

Det vil vere skilnader i kva opplysningar vi pliktar å gje, avhengig av om opplysningane er innsamla frå den registrerte sjølv, eller frå andre.

4.1 Kva inneber opplysningsplikta?

Opplysningsplikta inneber at kommunen på eige initiativ pliktar å gje den registrerte ei rekkje opplysningar når vi samlar inn personopplysningar om vedkomande. Opplysingsplikta gjeld både ved innsamling frå den registrerte (sjå definisjon over) eller frå andre, t.d. Folkeregisteret, NAV, politiet.

Innsamling av opplysningar om ein registrert kan til dømes skje ved hjelp av eit søknadsskjema, som skal fyllast ut av vedkomande, eller ved og utan førespurnad. Personopplysningar om den registrerte hentast både frå offentlege instansar og privat sektor (t.d. vandelsuttalar, likningsopplysningar).

Opplysningsplikta gjeld for alle registrerte som vi samlar inn, eller mottek personopplysningar om. Opplysninga gjeld også over for ein tredjemann, som ikkje er det opphavelege subjektet for innsamlinga av personopplysningar, men som er nemnt i opplysningane om den registrerte. Dette kan til dømes vere ektefelle, born, foreldre eller andre slektningar, ein profesjonell aktør, som lækjar eller psykolog m.m.

Kontroll av identitet

For at kommunen skal ivareta opplysningsplikta si, er det viktig at ein kontrollerer at vedkomande faktisk er den registrerte. Dette for å sikre at vi mellom anna overheld teieplikta vår, og ikkje gjev uvedkomande personar innsyn i ein registrert sine opplysningar. Sjå «generelt» for korleis sikre identitet.

4.2 Korleis oppfyller vi opplysningsplikta?

Kommunen skal gje den registrerte dei opplysningane vedkomande har krav på skriftleg.
Dette fordi det er viktig at vi dokumenterer at vi har oppfylt opplysningsplikta vår.

Kommunen må sikre at vedkomande vi gjev informasjon til, verkeleg er den registrerte.

Dersom den registrerte ber om å få informasjonen munnleg, er det viktig at vi sikrar dokumentasjon på at:

1) Kommunen har fått ein førespurnad om å gje opplysningane munnleg
2) Kommunen har sikra at vedkomande verkeleg er den registrerte
3) Kommunen har gitt opplysningane til den registrerte (lag eit notat eller påteikning på saka om kva informasjon vi har formidla, til kven og når).

For utsending av informasjon sjå «generelt» - utsending av informasjon.

Det er opp til kommunen å vurdere korleis informasjonen best kan formidlast til den registrerte. Dersom kommunen samlar inn personopplysningar via ein nettstad, kan vi gje den naudsynte informasjonen ved å nytte standardtekst i pop-up-meldingar som vert aktivert når den registrerte fyller ut skjema etc. Pop-up-meldingane kan innehalde lenkjer til underliggande informasjon i form av tekstar, videoar, lydfiler m.m, slik at ein registrert kan navigere til den informasjonen som er mest interessant og relevant for vedkomande.

Det er viktig at vi sikrar at informasjonen er tydelig framheva, og gjev den registrerte ei klar oversikt. Opplysningane vi pliktar å gje etter personvernlova skal vere tydeleg åtskilt frå annan informasjon.

For å gjere informasjonen meir forståeleg, kan vi supplere den skriftlege informasjonen med bilete, eller ikon som gjev betre oversikt for den registrerte. Informasjonen kan også gjevast gradvis t.d. ved utfylling av eit søknadsskjema.

4.3 På kva tidspunkt skal vi oppfylle opplysningsplikta?

Når personopplysingar kjem frå den registrerte sjølv
Personopplysningar er henta inn frå den registrerte, når vedkomande sjølv - anten på vår førespurnad, eller uoppmoda – gjev kommunen opplysningar.

I desse tilfella skal kommunen som utgangspunkt gje opplysningane samstundes med innsamlinga av opplysningane.

Er den registerte pålagd å fylle ut eit søknadsskjema eller anna skjema, kan informasjonen gjevast i sjølve søknaden eller i skjemaet.

Når den registrerte – t.d. uoppmoda – tek kontakt med kommunen, skal vi gje informasjonen snarast mogleg.

Vi skal alltid, vurdert opp mot den innsatsen som kravst, gi opplysningane så tidleg som mogleg. Normalt pliktar vi å gje informasjonen før, eller samstundes med innsamlinga av personopplysningar.

Merk! Vi pliktar berre å gje informasjonen ein gong, med mindre vi seinare skal behandle informasjonen til andre formål enn det ein opphaveleg har samla inn opplysingane til.

Når personopplysningar kjem frå andre enn den registrerte sjølv
Dette kan vere informasjon vi har innhenta frå offentlege kjelder, offentlege instansar, eller frå andre registrerte.

I desse tilfella, må vi gje opplysningane så tidleg som mogleg etter innsamlinga.

Det vil avhenge av omstenda i saka, når vi som behandlingsansvarleg pliktar å informere.
Vi skal alltid, vurdert opp mot den innsatsen som kravst, gje ut opplysningar så tidleg som mogleg. Normalt pliktar vi å gje informasjonen innan **10 dagar,** om vi ikkje gjev den samstundes med innsamlinga av personopplysningane.

Dersom ein på tidspunktet for innsamlinga av personopplysingar veit at ein innan kort tid skal ha kontakt med den registrerte, kan ein vente til dette tidspunkt med å gi opplysingane om innsamlinga.

Dersom personopplysningane skal vidareformidlast til ein tredjepart, kan du vente med å gje opplysninga til første gongen du vidareformidlar personopplysningane til denne tredjeparten.

Ein føresetnad for å nytte denne fristen, er at det på tidspunktet for innsamlinga er klart at du skal vidareformidle denne informasjonen til ein tredjepart.

NB! Informasjonen kan ikkje gjevast seinare enn 1 månad etter at vi har samla inn personopplysningane.

Informasjonen skal som hovudregel berre gjevast ein gong (inkludert ved fortløpande innsamling), med mindre du seinare behandlar personopplysningane til andre formål enn det du opphaveleg samla dei inn for.

Kva opplysningar pliktar vi å gje når personopplysningar er innhenta frå den registrerte sjølv

Kva informasjon skal vi alltid gje til den registrerte?
Når vi samlar inn personopplysningar frå den registrerte sjølv, skal den registrerte informerast om namnet på saksbehandlaren som har samla inn personopplysningane, og kontaktinformasjonen til denne.

Vidare skal vi informere om kven som er personvernombod og kontaktinformasjonen til ombodet.

Den registrerte skal vidare ha opplysningar om formålet for og rettsgrunnlaget for kommunen si behandling av personopplysningane (sjå «Rettleiing behandlingsgrunnlag for behandling av personopplysningar). Dersom kommunen i medhald av lovheimel har rett og plikt til å samle inn personopplysningar, må vi opplyse om kva lov dette er og kapittel og/eller paragraf.
Dersom behandlingsgrunnlag er basert på ei interesseavveiing (berettiga interesse), skal den registrerte ha opplysing om kva for interesse kommunen eller ein tredjepart vil oppfylle.

I dei høva der vi ved tidspunktet for innsamling veit at personopplysningane skal sendast vidare til andre som t.d. andre myndigheiter eller private selskap - må vi informere den registrerte om dette, og kva grunnlag vi har til å gjere det: t.d. lovheimel, samtykke, interesseavveiing.

Dersom personopplysningar skal overførast til eit land utanfor EU/ EØS, så utløyser dette ei plikt til å gje den registrerte ei rekkje opplysningar. For det første må vi opplyse om overføringa er til eit trygt eller usikkert tredjeland. I sistnemnte tilfelle må du også informere den registrerte om kva som er grunnlaget for overføringa. Dette vil ikkje oppstå ofte, men det kan vere tilfelle når vi nyttar «skyløsninger». Dersom problemstillinga dukkar opp bør du ta kontakt med personvernombodet.
Merk at overføring også omfattar det å gje tilgang til opplysningane til personar utanfor EU/EØS, til dømes ved vedlikehald av eit system. Det er tilstrekkeleg at den som ser opplysningane er i eit land utanfor EU/ EØS, sjølv om opplysningane er lagra i EU/ EØS.

Dersom det rettslege grunnlaget for behandlinga av personopplysingane er art 6 nr. 1 (e):

> e) *behandlingen er nødvendig for å utføre en oppgave i allmennhetens interesse eller utøve offentlig myndighet som den behandlingsansvarlige er pålagt,* eller (f):
>
> *f) behandlingen er nødvendig for formål knyttet til de berettigede interessene som forfølges av den behandlingsansvarlige eller en tredjepart, med mindre den registrertes interesser eller grunnleggende rettigheter og friheter går foran og krever vern av personopplysninger, særlig dersom den registrerte er et barn.*
>
> *Nr. 1 bokstav f) får ikke anvendelse på behandling som utføres av offentlige myndigheter som ledd i utførelsen av deres oppgaver*.

skal vi seinast ved tidspunktet for den første kommunikasjonen med den registrerte, gjere vedkomande merksam på retten til å protestere mot behandlinga av personopplysingane.

I tillegg må vi gje informasjon om kor lenge opplysningane skal lagrast. Informasjonen om dette bør vere så konkret som mogleg. Det må også opplysast om den registrerte sine rettar, som retten til innsyn, retting, sletting og avgrensing av behandlinga av personopplysningane. Sjå vedlagde mal «Underretning om innsamling av personopplysningar»

Dersom behandlinga av personopplysningar er basert på samtykke, pliktar vi å opplyse om at eit samtykke til ei kvar tid kan trekkjast attende. ***Sjå rettleiing «Rettsleg behandlingsgrunnlag for behandling av personopplysningar» - Særskilt om samtykke.***

Det må også å opplysast om at den registrerte kan klage til Datatilsynet om opplysingsplikta ikkje er overhalden.

Om ei behandling er basert på lov eller avtale, er det nødvendig å informere den registrerte om at vedkomande er forplikta til å gje personopplysningar grunna lovkrav, kontrakt eller liknande, og konsekvensane det vil ha å ikkje gje naudsynte opplysningar.

Dersom vi nyttar automatiserte avgjerder, inkludert profilering, bør vi spesielt vurdere å gje den registrerte opplysningar om logikken i denne typen behandling (der automatisering eller profilering skjer) og betydinga og forventa konsekvensar av slik behandling for den registrerte.

Dersom ein nyttar personopplysingane til andre formål enn det dei var innsamla til, skal vi informere om dette.

Unntak frå opplysningsplikta når personopplysningar er samla inn frå den registrerte sjølv
Dersom den registrerte allereie er kjent med opplysningane vi skal gje etter punkt 4.1, treng vi ikkje gje ytterligare informasjon. Vi må likevel kunne dokumentere:

- Kva opplysningar den registrerte har fått
- Korleis og når den registrerte har fått opplysningane
- At det ikkje har skjedd endringar i desse opplysningane, etter at den registrerte fekk dei.

Kva pliktar vi å opplyse om når personopplysningane er henta frå andre enn den registrerte sjølv (t.d. NAV, politi, barnevern)

Kva informasjon skal vi alltid gje til den registrerte?
Dette er i hovudsak den same informasjonen som vi pliktar å gje i dei høva der personopplysningane er gjevne av den registrete sjølv (sjå over). I tillegg må det alltid opplysast om retten til å klage til Datatilsynet.

Utover dette må vi også gje informasjon om kva kategoriar av personopplysningar vi har samla inn. Er det «vanlege personopplysningar» eller «sensitive personopplysningar», sjå definisjon av «sensitive personopplysningar» under punktet «Generelt».

Dessutan må vi gje ytterlegare opplysningar om rett til sletting, innsyn, retting, lagringstid m.m., tilsvarande som for dei høva der opplysningane kjem frå den registrerte sjølv.

Vi må også vurdere konkret om vi skal gje den registrerte informasjon om kvar personopplysningane kjem frå, og om dei stammar frå offentleg tilgjengelege kjelder.

Unntak frå opplysningsplikt når personopplysningane er henta frå andre enn den registrerte (t.d. NAV, politi, barnevern)

Vi har ikkje plikt til å gje opplysningar til den registrerte i desse høva:

- Dersom kommunen med heimel i lov er pålagt å samle inn eller vidareformidle personopplysningar
- Dersom den registrerte allereie er kjend med opplysningane vi pliktar å gje. Merk at ein registrert sjeldan vil vere kjend med opplysningane, ettersom kommunen har samla opplysningane frå andre enn den registrerte sjølv
- Dersom det er umogleg, eller det vil krevje ein uforholdsmessig innsats, eller hindre formålet med innsamlinga, om vi gjev opplysningar
- Dersom det ikkje på nokon måte er mogleg å identifisere kven den registrerte er. Merk at det er kommunen som må bevise at det er umogleg å oppfylle opplysningsplikta, og at vi kan måtte gje opplysningane på eit seinare tidspunkt, om det vert mogleg
- Dersom behandlinga av personopplysningar skjer til vitskaplege eller statistiske formål. Vi må her dokumentere at vilkåra for unntak i lova er oppfylt
- Ei underretting vil gjere det umogleg eller i alvorleg grad hindre oppfyllinga av formålet med behandlinga. Vi må her dokumentere at dette er tilfelle

Opplysningsplikta gjeld for alle registrerte personar vi samlar inn, eller får personopplysningar om. Dette kan også vere bi-personar, som ikkje er dei opphavelege subjekta for innsamlinga av personopplysningar. Dette kan til dømes vere ektefelle, born, foreldre eller andre slektningar, ein profesjonell aktør, som lækjar eller psykolog m.m. For desse vil du kunne nytte unntak frå opplysingsplikt, då ei oppfylling av opplysningsplikta ovanfor desse personane ofte vil vere umogleg, eller krevje ein uforholdsmessig stor innsats, i høve til den avgrensa rolla ein slik bi-person har for saka.

I dei tilfella vi vurderer at det vil krevje ein uforholdsmessig stor innsats å gje opplysningar til den registrerte, skal vi alltid vurdere om vi kan gje generell informasjon på kommunen si heimeside om innsamling av personopplysningar, ha opplysingskampanjar m.m.

Det er viktig å vere merksam på at vi ikkje plikter å opplyse om høve som er konfidensielle, i medhald av reglar om teieplikt m.m.

Generelt unntak frå opplysningsplikta etter personopplysningslova § 16:

I desse tilfella gjeld ikkje opplysningsplikta: *«§ 16.Unntak fra retten til informasjon og innsyn og plikten til underretning om brudd på personopplysningssikkerheten*

Retten til informasjon og innsyn etter personvernforordningen artikkel 13, 14 og 15 omfatter ikke opplysninger som

a) er av betydning for Norges utenrikspolitiske interesser eller nasjonale forsvars- og sikkerhetsinteresser, når den behandlingsansvarlige kan unnta opplysningene etter offentleglova §§ 20 eller 21

b) det er påkrevd å hemmeligholde av hensyn til forebygging, etterforskning, avsløring og rettslig forfølgning av straffbare handlinger

c) det må anses utilrådelig at den registrerte får kjennskap til av hensyn til vedkommendes helse eller forholdet til personer som står vedkommende nær

d) i lov eller med hjemmel i lov er underlagt taushetsplikt

e) utelukkende finnes i tekst som er utarbeidet for intern saksforberedelse, og som heller ikke er utlevert til andre, så langt det er nødvendig å nekte innsyn for å sikre forsvarlige interne avgjørelsesprosesser

f) det vil være i strid med åpenbare og grunnleggende private eller offentlige interesser å informere om.

Opplysninger som nevnt i første ledd bokstav c kan på anmodning likevel gjøres kjent for en representant for den registrerte når ikke særlige grunner taler mot det.

Den som nekter å gi innsyn i medhold av første ledd, må begrunne dette skriftlig og gi en presis henvisning til unntakshjemmelen. Dersom innsyn nektes på grunnlag av første ledd bokstav f, skal det også angis hvilke hensyn som begrunner hemmelighold.

Plikten til å underrette den registrerte om brudd på personopplysningssikkerheten etter personvernforordningen artikkel 34 gjelder ikke i den utstrekning en slik underretning vil røpe opplysninger som nevnt i første ledd bokstav a, b og d.

Kongen kan gi forskrift om unntak fra og nærmere vilkår for informasjons- og innsynsrett og underretning om brudd på personopplysningssikkerheten.»

Om behandling av personopplysningar til andre formål enn dei opphaveleg vart samla inn for
Dersom vi ønsker å nytte personopplysningar til eit anna formål enn det dei opphaveleg var samla inn for, inntrer opplysningsplikta på nytt.

Om det er lenge sidan vi sist ga informasjonen om den opphavelege behandlinga til den registrerte, bør vi vurdere om det er naudsynt å oppdatere informasjonen.

Ved vurderinga av kor lang tid i førevegen vi pliktar å gje den registrerte opplysningar må vi vurdere kor inngripande det endra formålet er for den registrerte. Dersom konklusjonen er at opplysningane er svært relevante og/ eller at behandlinga er særs inngripande for den registrerte, må vi gje opplysningane i god tid før vi byrjar på den nye behandlinga.

Ein standardmal for underretning til den registrerte om at vi har samla inn personopplysningar, ligg i kapittel Vedlegg.

5 Rutine ved krav om innsyn

«Lov om behandling av personopplysningar (personopplysningsloven) og forordning (EU) 2016/679 om personvern ART. 15

Denne rutinen gjeld når ein registrert ber om innsyn i kva personopplysningar kommunen behandlar om vedkomande. Rutinen omhandlar også kva opplysningar vil pliktar å gje den registrerte om vår behandling av vedkomande sine personopplysningar.

Innsynsretten er heimla i personvernlova § 1 og § 16 jf. personvernforordninga art. 15.
Merk at det er eigne innsynskrav etter forvaltningslova § 18, offentleglova § 3 og annan lovbestemt rett til innsyn.

Innsynsretten etter personopplysningslova gjeld ikkje for døde personar.

5.1 Kva inneber innsyn i personopplysningar?

Retten til innsyn inneber at den vi behandlar personopplysningane til som hovudregel har full innsynsrett i dei personopplysningane som kommunen behandlar om vedkomande. Innsynsretten gjeld også for utstrukturerte personopplysningar.
Sjå eiga rettleiing for utstrukturerte personopplysningar.

For born gjeld det innsynsretten for barnet sjølv, og for dei som har foreldreansvaret.

Formålet med innsynsretten er at den registrerte skal ha høve til å sjå kva personopplysningar kommunen behandlar om vedkomande, og skape openheit om kommunen si behandling av opplysningane. På bakgrunn av innsynet, kan den registrerte kontrollere at personopplysningane er korrekte og at dei vert lovleg behandla.

Vidare inneber retten til innsyn at den registrerte har krav på å få opplyst om korleis vi behandlar personopplysningane.

Kommunikasjon om innsyn skal som hovudregel skje skriftleg med mindre den registrerte spesifikt ber om eit munnleg svar. Ved munnleg saksbehandling, må vi sikre skriftleg dokumentasjon på kva vi har sagt og gjort.

Dersom eit krav er sendt elektronisk, per e-post eller Digital Post, skal kommunen svare på tilsvarande måte, om mogleg.
NB! Sensitive personopplysingar (sjå definisjon under punktet «Generelt»), skal ikkje sendast på e-post. Heller ikkje opplysingar som ved å kome på avvege, lett kan misbrukast, typisk fødsels- og personnummer og bankkontonummer.

Meldingar til den registrerte skal vere kortfatta, ha eit klårt og enkelt språk, vere lett tilgjengelege og lett forståelege. Dersom den registrerte er eit born, skal språket tilpassast i høve barnet sin alder og utvikling.

5.2 Førespurnad om innsyn

Den som ønskjer innsyn, skal rette ein formell førespurnad om dette til kommunen.

Førespurnaden skal helst sendast til kommunen via eDialog. I førespurnaden må det skildrast kva personopplysningar ein vil ha innsyn i og kven som skal motta dei.

Kven skal ha førespurnaden?
Det er arkivet som skal ta imot, koordinere og arkivere førespurnadar som gjeld innsyn. Personvernombodet skal straks informerast om førespurnadar.

Før vi kan overføre personopplysningane, må innsendar legitimere seg, sjå eige punkt om dette under «Generelt». Om eDialog vert nytta, er innsendaren allereie legitimert.

Kommunen kan ikkje nekte å behandle førespurnader som kjem per e-post, telefon, brev eller oppmøte, men merk punktet under «Generelt» om sikring av identitet.

Arkivet skal ta kontakt med den som på vegne av kommunen har ansvaret for det systemet ein har dei etterspurde opplysingane registrert i. Dette kan vere fleire system. Det vil avhenge av kva vedkomande ønskjer innsyn i. Merks at det også må undersøkast om vi har såkalla utstrukturerte personopplysningar (sjå eigen rettleiar om dette). Den ansvarlege lagar til ei oversikt over personopplysingane ev. kopi av dokument. **NB! Ved utlevering av heile dokument må ein sikre at ein sladdar opplysningar om andre personar.**

Dersom nokon ønskjer innsyn i korleis kommunen behandlar personopplysingar på generelt grunnlag, har vi utarbeidd protokoll(ar) over behandling av personopplysingar. Det er lenke til denne oversikta på kommunen si heimeside.

Kan vi be den registrerte om å presisere kravet om innsyn?
Dersom kommunen behandlar ei stor mengde opplysningar om ein person, kan vi be om at den registrerte presiserer kva opplysingar vedkomande ønskjer innsyn i. Dette kan også lette kommunen si saksbehandling, og på den måten forkorte saksbehandlingstida til fordel for den registrerte.

NB! Vi kan ikkje avvise eit krav om innsyn, om den registrerte ikkje ønskjer å presisere kravet sitt. Dette inneber at kommunen må gje ut alle personopplysningane vi har om vedkomande. Det kan vere at denne informasjonen må samlast inn frå fleire avdelingar. Kommunen kan gje den registrerte innsyn i fleire omgangar etter kvart som ein får inn informasjon frå forskjellige einingar.

Spesielt om krav om innsyn i opplysningar om born
Når det gjeld behandling av opplysningar om born, kan den som har foreldreansvaret krevje innsyn på barnet sine vegne. Merk at det ikkje utan vidare er slik at den med foreldreansvaret kan krevje innsyn når det gjeld større born. Det kan også vere høve der det berre er barnet, og ikkje dei med ansvaret, som bør få innsyn. Dette vil vere tilfelle der det er snakk om høve av særs privat og personleg karakter (t.d. abort).

Det er som oftast ingen grunn til å ikkje gje innsyn til personar under 18 år. Normalt må born sjølv kunne be om innsyn frå dei er omkring 13- 15 år.

Om eit born har kravd innsyn, inneber ikkje dette at kommunen kan nekte innsyn for den som har foreldreansvaret.

Kontroll av identitet
Når kommunen får eit krav om innsyn, er viktig at vi kontrollerer at den registrerte er rette vedkomande. Dette for å sikre at vi mellom anna overheld teieplikta vår og ikkje gjev uvedkomande personar innsyn i ein registrert sine opplysningar. Sjå «Generelt» for korleis sikre identitet

5.3 Svarfrist

Kommunen skal svare på eit krav om innsyn utan unødig forseinking og **seinast 1 månad** etter at vi har motteke kravet.

Om det er ei komplisert krav, kan fristen forlengjast med ytterlegare **2 månader**. Kommunen skal i slike høve gjere vedkomande merksam på forseinka saksbehandlingstid og grunngjevinga for dette, **seinast 1 månad etter mottak av kravet.**

ABSOLUTT FRIST for å svare på eit krav er på **3 månader**.

5.4 Avvising av eit innsynskrav

Den registrerte skal informerast om avvisinga straks, og **seinast 1 månad** etter kommunen har motteke innsynskravet.

Avslaget skal grunngjevast i medhald av forvaltningslova (t.d. kommunen behandlar ikkje opplysningar om personen) og kommunen pliktar å informere om høve til å klage til Datatilsynet, eller bringe saka inn for domstolane.

Openbert grunnlause eller overdrivne krav frå registrerte

I særlege tilfelle kan kommunen anten avvise eit krav frå ein registrert, eller krevje eit rimeleg gebyr for behandling av krav. Dette gjeld dersom eit krav er openbert grunnlaust, eller overdrive fordi det vert gjenteke. (t.d. den registrerte ved korte intervall krev innsyn i dei same opplysningane.)

NB! Kommunen som behandlingsansvarleg må bevise at eit krav frå ein registrert er openbert grunnlaust eller overdrive. Vi må vere sikre på at vi har dokumentasjon som underbyggjer at vi har grunnlag for å avvise kravet eller krevje gebyr.

Som offentleg myndigheit, har kommunen rettleiingsplikt etter forvaltningslova § 11, som inneber at vi bør gå i dialog med vedkomande for å avgrense kravet slik at det ikkje lenger er t.d. overdrive.

5.5 Kva opplysningar skal kommunen utlevere til den registrerte?

Det er innsyn i innhaldet av personopplysningane som kommunen behandlar, den registrerte skal ha innsyn i. Kommunen kan difor velje å gje ut kopiar av originale dokument, saksmapper, overvakingsbilete m.m. Men kommunen kan også kopiere opplysningane over i eit nytt dokument eller liknande.

5.6 Korleis gje innsyn?

Opplysningane skal sendast til den registrerte på ein sikker måte. Den registrerte må avtale korleis vedkommande vil ha overført sine personopplysningar. Døme: sikker digital post (KS SvarUT), minnepenn, Dropbox eller andre skylagringstenester, rekommandert post med meir.

NB! Sensitive personopplysingar (sjå definisjon under punktet «Generelt»), skal ikkje sendast på e-post. Heller ikkje opplysingar som ved å kome på avvege lett kan misbrukast, typisk fødsels- og personnummer og bankkontonummer.

Det er berre opplysningar om den registrerte sjølv, som skal utleverast. Om kopiane inneheld opplysningar om andre, skal desse opplysningane sladdast/ fjernast.

Som kommune må vi vurdere om innsyn etter forvaltningslova § 18 eller offentleglova § 3 vil vere meir gunstig for den registrerte. Merk at innsyn etter desse lovene som hovudregel skal skje innan 1-3 dagar.

Kommunen skal gje den registrerte ein gratis kopi av personopplysningane (med mindre kravet er openbert grunnlaust eller overdrive). Dersom den registrerte ønskjer fleire kopiar, kan kommunen krevje eit rimeleg gebyr basert på administrasjonskostnadane.
Mal til svarbrev ligg i kapittel Vedlegg.

Plikt til å gje ytterlegare opplysningar om den behandlinga kommunen gjer

I tillegg til innsyn i personopplysningane, skal vi også gje den registrerte ei rekkje opplysningar om sjølve behandlinga. Desse opplysningane kan gjevast i eit eige følgjebrev, men skal sendast samstundes med personopplysningane.

Opplysningane vi pliktar å gje den registrerte er:

1. Formålet med behandlinga av personopplysningane – kvifor har kommunen desse opplysningane om vedkomande.
2. Kategoriar av personopplysningar (alminnelege opplysningar, sensitive personopplysningar)
3. Mottakarar eller kategoriar av mottakarar (kven vil opplysningane verte vidareformidla til t.d. politiet, skatteetaten, andre offentlege eller private institusjonar?)
4. Mottakarar i tredjeland, derunder internasjonale organisasjonar (viss dette er gjort må vi informere den registrerte om at vi har oppfylt dei garantiane som lovverket krev for slik overføring). Sjeldan aktuelt for kommunen.
5. Korleis vi oppbevarer personopplysningane – og om mogleg kor lenge det forventast at personopplysningane vert lagra. Om dette ikkje er mogleg, kriteria som vert nytta for å fastsetje denne perioden som t.d. arkivlova m.m.
6. Kvar personopplysningane kjem i frå (berre opplyse om dette dersom opplysningane kjem frå andre enn den registrerte sjølv)?
7. Automatiske avgjerder, derunder profilering (må informere om at kommunen har gjort ei slik behandling, samt logikken i dei automatiserte avgjerdene. Kva vurderingar ligg til grunn for behandlinga, og korleis kjem systemet fram til avgjerdene)
8. Rett til korrigering, sletting, avgrensa behandling og protest. Den registrerte skal informerast om at han/ ho har rett til å krevje retting, sletting, avgrensing av behandlinga og har rett til å kome med protestar mot behandlinga i enkelte situasjonar)
9. Klage til Datatilsynet – vi pliktar å informere om at den registrerte kan klage på behandlinga til Datatilsynet

Unntak frå innsynsretten etter GDPR Art.15 (4) og personopplysningslova § 16

Forordninga Art. 15 (4):

Dersom det å imøtekome eit innsynskrav vil krenkje andre sine rettar og fridom.

Personopplysningslova § 16: LOV-2018-06-15-38 Lov om behandling av personopplysninger:

a) når det er av betyding for riket si sikkerheit

b) det er påkravd å halde opplysningane hemmelege av omsyn til førebygging, etterforsking, avsløring og rettslig forfølgning av straffbare handlingar

c) det ikkje er tilrådd at den registrerte får opplysningane av omsyn til vedkomandes helse eller av omsyn til nærståande personar

d) opplysninga er underlagt teieplikt

e) når opplysningane berre eksisterer i tekst som er utarbeidd for vår interne saksførebuing og det er naudsynt å nekte innsyn for å sikre forvarlege interne sakshandsamingsprosessar

f) det vil være i strid med openbare og grunnleggande private eller offentlige interesser å informere om opplysningane

Merk at kommunen her berre kan unngå å ta med dei opplysningane som vil innebere ei krenking av slike rettar, og at den registrerte har krav på alle andre opplysningar.

6 Rutine ved krav om sletting, korrigering eller avgrensa behandling av personopplysningar

LOV-2018-06-15-38 Lov om behandling av personopplysninger og personvernforordning art. 16, 17 18 nr.1.

Denne rutinen gjeld der ein person (den registrerte) ber om å få sletta, korrigert eller avgrensa behandling av personopplysningar.

Kva inneber sletting av personopplysningar?

Retten til sletting er heimla i personopplysingslova § 1 jf. personvernforordning art. 17.

Den registrerte skal ha rett til å få sletta opplysingar om seg sjølv utan ugrunna opphald dersom:

- formålet med behandlinga av personopplysingane er innfridd
- den registrerte trekk tilbake sitt samtykke for behandling av personopplysingar, og det ikkje ligg føre noko anna behandlingsgrunnlag
- den registrerte har protestert mot behandlinga, og det ikkje finns meir tungtvegande, kvalifiserte grunnar til fortsatt behandling av personopplysningar. Dette gjeld også om opplysingane vert brukt i marknadsføring
- personopplysingane vert behandla ulovleg
- personopplysingane må slettast for å oppfylle ei rettsleg forplikting etter unionsretten eller norsk rett som kommunen er underlagt
- opplysingane er samla inn i samband med informasjonstenester basert på samtykke frå born. Eller den med foreldreansvar for barnet og den registrerte tilbakekallar samtykke. (frå 13 år)

Retten til sletting inneber at den registrerte har rett til å få sletta opplysingar om seg sjølv på ein slik måte at dei ikkje kan attskapast. Dette vil seie at vi også skal slette opplysingane frå t.d. datatryggleikskopiar osv. viss dette er teknisk mogleg. Under alle omstende skal vi sikre seg at dersom vi nyttar data frå ein tryggleikskopi, så skal vi fjerne opplysingar som er sletta frå det «aktive» systemet.

Retten til sletting betyr at vi berre skal behandle opplysingar som har eit formål.
Når formålet er innfridd, har ein normalt ikkje rett til å behandle opplysingane lenger og dei skal difor slettast.

Dette er i tråd med prinsippet om dataminimering som er heimla i Personvernforordninga art. 5.
Kommunen som behandlingsansvarlege, uavhengig av den registrerte sin rett til sletting, vil vere forplikta til å slette personopplysingar når formålet er innfridd.
Kvar enkelt fagsystem skal ha rutinar for lagring og sletting.

Kommunen er underlagt arkivlova, rekneskapslova, og andre særlover, som gjer at vi ikkje alltid kan slette personopplysingar.

Dette vil seie at krav om sletting av personopplysingar i all hovudsak vil gjelde opplysingar som kommunen sjølv skal slette, men at ein ikkje har kome til det tidspunkt der det er gjort.
Det omfattar også ustrukturerte data, som til dømes opplysningar som ligg i e-postar, filer, katalogar eller excel-ark.

Unntak frå retten til sletting
Art. 17 listar opp ein del situasjonar der kommunen ikkje er forplikta til å slette personopplysingar. Dette er tilfelle der kommunen må behandle personopplysingane for å:

a) utøve retten til ytrings- og informasjonsfridom
b) overhalde ei rettsleg forplikting
c) utføre ei oppgåve i samfunnet si interesse
d) utføre offentleg myndigheit som kommunen er pålagt

Dette betyr at ei kommune – som offentleg myndigheit – ikkje er forplikta til å slette opplysningar etter forordninga dersom andre reglar seier at ein ikkje må slette dei, t.d. arkivlova og rekneskapslova. Arkivlova gir i svært få tilfelle offentleg myndigheit rett til å slette dokument.

Vi er heller ikkje forplikta til å slette personopplysningane dersom behandlinga av personopplysingane er naudsynt av omsyn til ålmenta si interesse på området folkehelse, samt av omsyn til formål knytt til vitskaplege eller historisk forsking, eller for statistiske formål.

Kommunen er heller ikkje forplikta til å slette personopplysningane dersom vidare behandling er naudsynt for å fastsetje, gjere gjeldande eller forsvare rettskrav. Dette vil seie at vi vil kunne fortsetje å behandle opplysingar dersom dei skal nyttast i ei rettssak. Dette kan t.d. vere tilfelle for personopplysingar i t.d sak om mobbing, eller tvist i kontraktsforhold.

I dei tilfella der opplysningane ikkje kan slettast, skal dette grunngjevast og leggast inn i saka slik at dette er opplyst og dokumentert.
Den registrerte sitt krav om sletting skal også leggast inn i saka.

Korrigering av personopplysningar

Retten til korrigering er heimla i Personopplysningslova §1 jf. Personvernforordning art. 16.

Kva inneber korrigering av personopplysningar?
Retten til korrigering betyr at den registrerte som hovudregel har rett til å få korrigert feilaktige opplysingar om seg sjølv. Ufullstendige opplysingar har ein rett til å få komplettert. Dette kan skje ved at den registrerte legg fram ei supplerande erklæring.
Den registrerte sin rett til å få komplettert ufullstendige opplysingar, betyr at vi ikkje kan avvise å supplere ein kategori opplysingar med ein annan kategori av opplysingar, så lenge opplysingane er relevante for å innfri formålet med behandlinga.

Formålet med retten til korrigering er at kommunen skal behandle opplysingar som er korrekte og oppdaterte, slik at t.d. vedtak vert fatta på rett grunnlag, og ein får rett teneste.
Dette er i tråd med prinsippet om integritet som er heimla i Personvernforordninga art. 5.

Sjølv om den registrerte har rett til å korrigere sine personopplysingar, endrar ikkje det på den kommunen si plikt etter forvaltningsretten til å på eige initiativ sørge for at opplysingane vi behandlar ervere korrekte og oppdaterte.

Avgrensa behandling av personopplysningar

Kva inneber avgrensa behandling av personopplysningar?
Avgrensa behandling er i forordninga sin artikkel 4 nr. 3 definert slik:
«merking av lagra personopplysningar med det som mål å avgrense behandling av desse i framtida».

Retten til å be om avgrensa behandling gjeld i desse tilfella:

a) Opplysningane si riktigheit er omtvista, til dømes der den registrerte og kommunen ikkje er samde om sletting / korrigering.
b) Behandlinga er ulovleg og den registrerte ikkje vil be om sletting av personopplysningar, og i staden ber om avgrensa behandling.
c) Behandlinga ikkje lenger er naudsynt , men opplysningane trengs for å fastsetje, gjere gjeldande eller forsvare eit rettskrav
d) Den registrerte har protestert mot vidare behandling, jf. art 21 nr.1, og i vente på ei avgjerd ber den registrerte om avgrensa behandling.

Dersom eit av desse vilkåra er oppfylt, har kommunen berre rett til å behandle dei aktuelle personopplysningane (bortsett frå lagring) dersom den registrerte samtykker, eller dersom det er naudsynt for å fastsetje, gjere gjeldande eller forsvare eit rettskrav eller verne ein anna fysisk eller juridisk person sine rettar eller viktige ålmente interesser.

Dersom avgrensa behandling ikkje lenger er aktuelt, skal den registrerte underrettast av kommunen før avgrensinga opphevast.

6.1 Førespurnad om sletting, korrigering eller avgrensa behandling

Den som ønsker sletting, korrigering eller avgrensa behandling skal rette ein formell førespurnad om dette til kommunen.

Førespurnaden skal som hovudregel sendast til kommunen via eDialog.
I førespurnaden må det skildrast kva personopplysningar ein ønsker sletta, korrigert eller avgrensa behandling av.

Kven skal ha førespurnaden?
Det er arkivet som skal ta i mot, koordinere og arkivere førespurnadar som gjeld sletting, korrigering eller avgrensa behandling. Personvernombodet skal straks informerast om førespurnadar.

Før vi kan behandle førespurnaden, må innsendar legitimere seg (sjå eige punkt om dette under «Generelt»).
Viss eDialog vert nytta, er innsendaren allereie legitimert.

Meldingar til den registrerte skal vere kortfatta, lett tilgjengelege og lett forståelege. Språket skal vere klårt og enkelt. Dersom den registrerte er eit born, skal språket tilpassast barnet sin alder og utvikling.

Arkivleiar skal kontaktast for å sikre at reglane i arkivlova ikkje vert brotne.

Spesielt ved krav om sletting, korrigering eller avgrensa behandling av opplysningar om born
Når det gjeld behandling av opplysningar om born, kan den som har foreldreansvaret krevje dette på barnet sine vegne.

6.2 Korleis korrigere personopplysingar?

Korrigering når det er semje mellom kommunen og den registrerte om at opplysingane skal korrigerast

Som offentleg myndigheit er kommunen forplikta til å dokumentere det grunnlag ein fattar vedtak på. Dette vil seie at vi ikkje automatisk skal fjerne dei ukorrekte opplysingane.

Vi korrigerer opplysingane ved å tilføre dei korrekte opplysingane i saka, utan å samstundes fjerne dei opplysningane som er ukorrekte. Det er viktig at det kjem klårt fram kva som er korrekte opplysingar i saka, og at opplysingane er korrigert. Dette kan t.d. gjerast ved å sette inn ei tilvising til dei ukorrekte opplysingane. Husk også å slett dei korrigerte opplysningane som ligg i ustrukturerte data.

Korrigering når det ikkje er semje mellom kommunen og den registrerte om at opplysingane skal korrigerast

Er saksbehandlar i kommunen ikkje samd i at opplysingane om den registrerte er ukorrekte, pliktar ikkje kommunen å korrigere dei.

Usemja kan t.d. gå på kva som vart sagt i eit møte eller opplysingar i eit notat om besøk i heimen.

Sjølv om vedkomande saksbehandlar ikkje er samd i den registrerte sine synspunkt, skal vi sørgje for at dei personopplysingane vi behandlar er korrekte og fullstendige.

I slike tilfelle skal ein difor sørgje for at det vert laga eit tilføying til dei omstridde opplysingane der det framkjem at den registrerte ikkje er einig i at opplysingane er korrekte, og kva han eller ho meiner er korrekte opplysingar.

Ein er altså i slike situasjonar ikkje forplikta til å korrigere opplysingane dersom det er vedkomande saksbehandlar si saklege oppfatning at dei er korrekte.

Korrigering når det gjeld opplysingar som har karakter av ei subjektiv eller fagleg vurdering
I mange tilfelle inneheld saker faglege eller subjektive vurderingar om ein registrert. Dersom ein registrert er usamd i desse opplysingane, vil det ofte vere vanskeleg å fastslå om opplysingane er korrekte eller ikkje. Løysninga i slike situasjonar vil derfor normalt vere å tilføre opplysingar om den registrerte sitt synspunkt i saka. Dersom opplysningane ligg som ustrukturerte data er det viktig å snarast sørge for å overføre opplysningane, både dei opphavelege og dei nye, til aktuelt saksbehandlingssystem.

Det kan og vere tilfelle at den registrerte har innhenta ei erklæring frå ein annan spesialist, og vedkomande har kome til eit anna resultat enn kommunen sin sakkunnige, t.d. legeerklæring.
Då legg ein ved erklæringa i saka utan å slette den førre vurderinga.

6.3 Svarfrist

Kommunen skal svare på eit krav om sletting, korrigering eller avgrensa behandling utan unødig forseinking og **seinast 1 månad** etter at vi har fått kravet.

Om det er eit komplisert krav, kan fristen forlengjast med ytterlegare **2** månader.
Kommunen skal gjere vedkomande merksam på forseinka saksbehandlingstid, og grunngjevinga for dette **seinast 1 månad etter mottak av kravet.**
ABSOLUTT FRIST for å svare på eit krav er på 3 månader.

6.4 Plikt til å informere eventuelle mottakarar

Kommunen som behandlingsansvarleg skal, i tillegg til å slette, korrigere eller behandle opplysingane avgrensa, på eige initiativ underrette dei vi eventuelt har sendt / vidareformidla dei ukorrekte opplysingane til. Dette følgjer av personvernforordninga art. 19.

Kommunen skal opplyse om kva som er korrigert / sletta eller om kva den avgrensa behandlinga gjeld.

Dersom vi har offentleggjort opplysingane, blir informasjonsplikta etter art. 19 forsterka, jf. Art. 17, nr. 2. Då skal vi innanfor rimelege rammer, treffe rimelege og om naudsynt, tekniske tiltak for å underrette mottakar om at den registrerte har bedt om sletting.
Dette inneber også alle lenkjer, kopiar og reproduksjonar.

Vi skal informere mottakarar, som fortsatt behandlar personopplysingane, om at den registrerte har kravd sletting, korrigering eller avgrensa behandling av dei aktuelle personopplysingane.

Plikta til å underrette ev. mottakarar gjeld ikkje dersom dette vil vere umogleg eller urimeleg vanskeleg. Då ei slik underretting ofte ikkje vil vere forbunde med store arbeidsmessige eller ressurskrevjande belastningar, og det i tillegg vil vere av stor betyding for den registrerte å få korrigert opplysingane, skal det tungtvegande grunnar til før ei kommune kan unnlate å informere ein mottakar

Dersom kommunen som behandlingsansvarleg mottek ei slik melding som nemnt over, skal vi vurdere om vi pliktar å slette opplysingane, eller om vi fortsatt kan behandle dei lovleg, altså med eit formål og behandlingsgrunnlag.

6.5 Svar på krav om sletting, korrigering eller avgrensa behandling

Saksbehandlar sender svar på om opplysingane vert sletta, korrigert eller om behandlinga vert avgrensa til den registrerte. Dette kan skje t.d. via Digital Post.

NB! Sensitive personopplysningar skal ikkje sendast på e-post.
Sjå «Generelt» for definisjon av sensitive personopplysningar.
Ein skal heller ikkje sende opplysingar som ved å kome på avvege kan misbrukast, typisk fødselsnummer og bankkontonummer.

Stadfesting kan også sendast i rekommandert post.

Sjå mal til svarbrev i kapittel Vedlegg.

7 Rutine ved protest mot behandling av personopplysningar i kommunen

Retten til å protestere mot behandling av personopplysningar er heimla i personopplysningslova §1 jf. personvernforordninga art. 21.

Retten til å ikkje vere gjenstand for automatisert behandling i nærare definerte tilfelle, er heimla i personopplysningslova i §1, jf. personvernforordninga art.22.

Kva inneber retten til å protestere mot behandling av personopplysningar?

Den registrerte har til ei kvar tid rett til å protestere mot behandling av sine personopplysningar når kommunen behandlar opplysningane på grunnlag av art. 6 nr 1 e og f («Behandlingen er nødvendig for å utføre en oppgave i allmenhetens interesse eller utøve offentlig myndighet som den behandlingsansvarlige er pålagt»).
Dersom du er i tvil om behandlingsgrunnlaget, sjå i behandlingsprotokollen.

Den registrerte har også rett til å protestere mot behandling av personopplysningar dersom dei blir behandla på grunnlag av automatisert behandling. Vidare har den registrerte også rett til å protestere om personopplysningane skal behandlast for vitskapelege eller historiske forskingsformål eller for statistiske formål, med mindre behandlinga er naudsynt for å utføre ein oppgåve i ålmenta si interesse.

Dersom den registrerte protesterer mot behandling av personopplysningar, må kommunen gjere ei skriftleg vurdering av om det er tvingande nødvendig å behandle desse opplysningane eller ikkje. Dersom behandlinga av personopplysningar er til vitskapeleg eller statistiske formål, må ålmenta sine interesser vere viktigare enn den registrerte sine interesser.

Ved ein protest skal kommunen som hovudregel stoppe all behandling av personopplysningane. Behandlinga kan likevel halde fram om det er tvingande berettiga grunnar for behandlinga, som går framfor den registrerte sine rettar til personvern, eller for å fastsette/ gjere gjeldande eller forsvare eit rettskrav.

Protest mot behandling av personopplysningar
Den som protesterer mot behandling av personopplysningane sine, skal som hovudregel gjere det skriftleg.

Protestar som kjem pr. e-post og telefon skal også bli behandla. Det skal vere avklart at protesten kjem frå den registrerte, sjå punktet «Generelt» om å sikre identitet.

Spesielt om protestar som gjeld opplysningar om born
Når det gjeld *behandling* av opplysningar om born, kan den som har foreldreansvaret protestere på barnet sine vegne.

Kontroll av identitet
Sjå «Generelt» for korleis sikre identitet

Svarfrist
Protestar skal behandlast så raskt som mogeleg.

Vanleg svarfrist på ein protest mot behandling av personopplysningar er **seinast 1 månad** etter at kommunen har motteke kravet.

Om det er eit komplisert krav, kan fristen forlengjast med ytterlegare **2** månader. Vil behandlinga ta meir enn ein månad, skal den som protesterer få underretning om den forseinka saksbehandlingstida og grunngjevinga for dette **seinast 1 månad etter mottak av kravet.**

ABSOLUTT FRIST for å svare på eit krav er på 3 månader.

Meldingar til den registrerte skal vere kortfatta, lett tilgjengelege og lett forståelege. Språket skal vere klårt og enkelt. Dersom den registrerte er eit born, skal språket tilpassast barnet sin alder og utvikling.

8 Bruk av bilete ogfilm

Skal du bruke bilete på til dømes heimesider, Intranett, Facebook, årsplanar, plakatar og andre informasjonsskriv frå kommunen?

Merk at dette er å rekne som behandling av personopplysningar.

Som hovudregel skal ein alltid be om samtykke for behandling av personopplysningar gjennom bilete og film. Merk at eit samtykke må dekke alle behandlingsaktivitetane!
Sjå rettleiing «Rettsleg behandlingsgrunnlag for behandling av personopplysningar» - Særskilt om samtykke.

Det er du som brukar bilete/ filmen som pliktar å vurdere om det er lovleg å offentleggjere dette.

Behandlingsaktivitetar:
Når det gjeld behandling av personopplysingar ved bruk av bilete, skjer det fleire behandlingsaktivitetar, som til dømes:

- Ta bilete
- Lagre bilete på kamera
- Overføre bilete til PC
- Lagre bilete på PC
- Publisere bilete på Facebook, aviser, nettside, brosjyre, dokument som vert distribuert
- Publisere med eller utan fullt namn
- Lagre bilete på maskina etter bruk

For barnehage/ skule: Gje ut bilete til føresette på minnepenn eller utskrift, når barnet sluttar i barnehagen/ skule. Dette kan også inkludere bilete av andre born.

Dersom eit samtykke skal vere gyldig, må ein samtykke til alle behandlingsaktivitetane.

Vi kan skilje mellom situasjonsbilete og portrettbilete

Situasjonsbilete: der ein aktivitet eller situasjon er det eigentlege formålet med bilete.
Kven som er med på biletet er mindre viktig enn hovudinnhaldet i biletet.
Det kan til dømes vere ei gruppe menneske på ein konsert, eit idrettsarrangement, 17.-mai tog, born i ein skulegard eller hendingar som har ålment interesse.

Situasjonsbilete **kan** offentleggjerast utan samtykke frå dei som er avbilda, så lenge bileta er harmlause og ikkje på nokon måte krenkjer dei som er avbilda.

Når det gjeld bilete av krenkande situasjonar eller meir spesielle høve, til dømes der ein ser pasientar på eit legekontor, personar i eit badeanlegg eller på ei strand, så skal desse normalt ikkje delast utan samtykke.

Portrettbilete: formålet med biletet er ein eller fleire bestemte personar. Det kan til dømes vere eit skulebilete eller eit klassebilete.

Dersom du skal publisere slike bilete på Internett-/papirpublikasjonar, eller dele dei med andre sjølv om det er i lukka grupper, må du ha samtykke frå den eller dei som er avbilda før biletet blir publisert. Dette personvernet gjeld så lenge den avbilda lever, og 15 år etter at vedkomande er død (åndsverklova -§45 c). Dette gjeld også film/video, og anten du har tatt biletet eller berre vidareformidlar det.

Klassebilete er også definert som portrettbilete, sidan det er personane som er hovudmotivet. Dersom ein skule ynskjer å publisere klassebilete på sine heimesider, kan dette berre gjerast dersom det er innhenta eit godkjent samtykke frå alle på bilete.

Det kan av og til vere vanskeleg å avgjere kva som er eit situasjonsbilete og portrettbilete, eller om situasjonen kan vere krenkande for nokon.
Som hovudregel bør ein difor alltid be om samtykke, dersom bilete eller filmar skal delast.

Samtykke skal hentast inn <u>før</u> offentleggjering/publisering av bilete/film.

<u>Særskilt om born og unge:</u>
Vi skal vere spesielt merksame på at born og unge har eit særleg personvern etter det nye regelverket. Når vi vurderer om publisering av bilete av born og unge er lovleg, må vi ta i betraktning at dei er mindre bevisste på risikoar og konsekvensar knytt til behandling av personopplysningar.

Dersom det gjeld barn eller andre personar som ikkje sjølv kan gje eit gyldig samtykke, må dei som har foreldreansvaret, eller verje gje samtykke på deira vegne.
Det er særs viktig å vise ekstra stor varsemd ved publisering av bilete og filmar av born.
Det er viktig at dei føresette får <u>god nok informasjon</u> før dei vert bedne om å samtykke til fotografering og eventuell publisering på nett, med eller utan fullt namn.

9 Ustrukturerte personopplysningar

Behandling etter personopplysningslova og personvernsforordninga art. 5

Formålet med rettleiinga er å forklare:

1. Kva er ustrukturerte personopplysningar?
2. Nærare om krava til behandling av ustrukturerte personopplysningar
3. Innsyn i ustrukturerte personopplysningar
4. Sletting av ustrukturerte personopplysningar

Kva er ustrukturerte personopplysningar?
Etter personvernlova og personvernforordninga kan ikkje kommunen innhente personopplysningar utan at det ligg føre eit konkret formål og eit rettsleg grunnlag.

For meir informasjon om regelverket sjå personvernforordninga (forordning (EU) 2016/679 av 27. april 2016 om beskyttelse av enkeltpersoner med omsyn til behandling av personopplysningar og om fri utveksling av slik informasjon) kap. 1 og 2.

Med ustrukturerte personopplysningar meiner vi personopplysningar som ikkje er lagra/oppbevart i eit søkbart system, eller der vi tek vare på opplysningane.
Søkbare system er både elektroniske system og papirarkiv.

Ustrukturerte personopplysningar kan til dømes vere:

- E-post
- Dokument lagra i filstruktur på den enkelte sin PC
- Papirdokument som ligg på kontoret
- Lydfiler
- Overvåkingsvideoar
- Sharepoint-dokument
- Google-skjema
- Bileter på jobbtelefon
- SMS/MMS

Personopplysningane som er lagra ustrukturert i kommunane, er ofte lagra på felles filområder eller i heimeområder på kommunalt datanettverk: Opplysningane kan vere sendt til private maskiner, i eigne skytenester eller på server for e-post.

Meir om krava til behandling av ustrukturerte personopplysningar
Personopplysningar skal som hovudregel ikkje oppbevarast som utstrukturerte data, men oppbevarast i strukturerte system, dersom vi har behov og behandlingsgrunnlag for å ta vare på opplysningane. Når data er flytta over i eit strukturert system, skal opplysningane ikkje ligge igjen i til dømes e-post. Dersom vi ikkje skal oppbevare personopplysningane, skal dei slettast, jamfør rutine for sletting.

Dersom personopplysningar likevel blir oppbevart som ustrukturerte data, skal dei vere oppbevart forsvarleg. Det skal dokumenterast behov for å ha personopplysningar som ustrukturerte data. Grunnlaget for å ha opplysningane skal vere innan ramma for reglane ipersonopplysningslova/personvernforordninga.
Ustrukturerte personopplysningar skal ikkje oppbevarast som ustrukturert informasjon lenger enn det er absolutt naudsynt i samband med saksbehandling.

Sensitive personopplysningar skal alltid oppbevarast i eit strukturert system med streng tilgangsstyring. Dei skal altså ikkje ligge i fellesmapper, heimekatalogar, e-post, lause dokument eller på skrivebord.

Innsyn i ustrukturerte personopplysningar
Ved krav om innsyn i personopplysningar, gjeld dette også innsyn i ustrukturerte data.
Når det kjem krav om innsyn skal ein følgje rutine for innsyn.

Dei nye personvernreglane krev at du i løpet av ein månad skal kunne gje fullstendig oversikt til ein person (den registrerte) over kva personopplysningar kommunen behandlar om vedkomande. Det vil krevje full kontroll på alle typar personopplysningar.

Sletting av ustrukturerte personopplysningar
Leiar er ansvarleg for å følgje opp at ustrukturerte personopplysningar blir sletta.
Ein kvar tilsett er sjølv ansvarleg for å slette ustrukturerte personopplysningar som han/ho oppbevarer. Sjå sjekkliste.

9.1 Sjekkliste – Ustrukturerte personopplysningar

Kontrollspørsmål:	**Dine svar:**
Oppbevarer eg ustrukturerte personopplysningar?	
Kva typar ustrukturerte personopplysningar oppbevarar eg?	
Korleis vert personopplysningane oppbevart?	
Kven har tilgang til personopplysningane?	
Har eg personopplysningar som skal leggjast over i eit strukturert system?	
Er eg kjend med rutinar for innsyn?	
Er eg kjend med rutinar for sletting?	

10 Rutine for sikkerheitsbrot på personvern

Det har skjedd eit brot på personvernsikkerheita, kva gjer vi som behandlingsansvarleg?

Det er eit brot på personvernsikkerheita dersom det fører til utilsikta eller ulovleg sletting, tap, endring, ulovleg spreiing av eller tilgang til personopplysningar som er overført, lagra eller på anna måte behandla.

Dette må gjerast etter at eit brot på personvernsikkerheita er oppdaga:

- Varsle personvernombodet umiddelbart
- Foreta ei konkret risikovurdering spesifikt i forhold til konsekvensane av brotet på personvernsikkerheita
- Vurdere om brotet krev underretning av den registrerte
- Melde frå om brotet til Datatilsynet innan 72 timar
- Dokumentere brotet, dei faktiske omstenda rundt brotet, konsekvens og tiltak som er gjort

Som utgangspunkt skal alle brot på personvernsikkerheita meldast til Datatilsynet.
Det er berre dersom det er usannsynleg at brotet inneber ein risiko for fysiske personar sine rettar og fridom, at det ikkje skal meldast inn til Datatilsynet.

Utfyllande informasjon om dei ulike punkta finn du lenger nede i rutinen.

Risikovurdering av brot
Risikovurderinga skal ta utgangspunkt i risikoen som har oppstått for dei aktuelle personane som følgje av eit brot på personvernsikkerheita.

- Type brot, om det er skjedd tap av opplysningar, brot på fortrulegheita eller integriteten.
    - Omfanget til opplysningane
    - Risikoen for at den registrerte kan identifiserast
    - Konsekvensar brotet kan ha for den registrerte
- Om brotet omfattar særlege tilhøve ved den registrerte, som til dømes dersom det er snakk om born eller særleg utsette.
- Talet på dei aktuelle fysiske personane

Vurdere om brotet krev underretning av den registrerte
Dersom det er sannsynleg at brotet på personvernsikkerheita vil medføre ein høg risiko for fysiske personar sine rettar og fridom, skal den behandlingsansvarlege utan ugrunna opphald underrette den registrerte om brotet.

Når den behandlingsansvarlege skal foreta ei risikovurdering, bør alle dei moglege konsekvensane og negative verknadane for den registrerte takast med i vurderinga. Dette omfattar såleis også dei «sekundære» konsekvensane for dei registrerte, som eit brot på personvernsikkerheita kan medføre.

Den behandlingsansvarlege skal i utgangspunktet alltid underrette den registrerte, uansett antal registrerte som er råka av brotet.

Melde frå om brotet til Datatilsynet
Det må delegerast løyve til gitte personar hos behandlingsansvarleg, som kan melde brot til

Datatilsynet.
Meldinga til Datatilsynet skal som eit minimum:

- Skildre karakteren av brotet på personvernsikkerheita, også dersom det er mogleg kategoriane og det omtrentlege talet på dei aktuelle registrerte, samt kategoriane og det omtrentlege talet aktuelle registreringar av personopplysningar.
- Angi namn på og kontaktopplysningar til Personvernombodet eller eit anna kontaktpunkt der det kan hentast inn fleire opplysningar.
- Skildre dei sannsynlege konsekvensane av brotet på personvernsikkerheita.
- Skildre dei tiltaka som den behandlingsansvarlege har gjort eller foreslått å gjere, for å handtere brotet på personvernsikkerheita, også nødvendige tiltak for å avgrense moglege skadelege effektar.
- Andre opplysningar dersom det er formålstenleg.

Dokumentasjon av brotet
Dokumentasjon av brot på personvernsikkerheita skal gjerast også dersom ein ikkje treng å melde brotet til Datatilsynet.

10.1 Kva er brot på personvern?

For å kunne handtere eit brot på personvern, skal den behandlingsansvarlege fyrst vere i stand til å forstå og kjenne igjen eit brot.
Eit brot på personvern vert i personvernforordninga art. 4 punkt 12 definert slik:

> *«brot på personopplysningssikkerheita er eit brot på sikkerheita som fører til utilsikta eller ulovleg sletting, tap, endring, ulovlig spreiing av eller tilgang til personopplysningar som er overført, lagra eller på anna måte behandla»*

Eit brot på personvern er samtidig eit informasjonssikkerheitsbrot.
DIFI legg følgjande innhald i omgrepet informasjonssikkerheitsbrot:

> *«Informasjonssikkerheitsbrot er brot på konfidensialitet, integritet og/eller tilgjengelegheit. Brotet kan ha store, små eller ingen konsekvensar»*

Berre dei sikkerheitshendingane som fører til utilsikta eller ulovleg sletting, tap, endring, uautorisert utlevering av eller tilgang til personopplysningar, er omfatta av personvernforordninga sin definisjon av eit brot på personvern.

Ei sikkerheitshending vil ikkje alltid vere eit brot på personvernet. Eit døme her kan vere fleire nyttelause forsøk på innlogging, som vil vere å betrakte som ei sikkerheitshending utan at det samtidig er brot på personvernet.

Ulike typar brot på personvernet

Eit brot på personvernet kan skje på fleire ulike måtar. Det kan t.d. skje ved teknisk-, menneskeleg- eller rutinesvikt.

Døme på brot på personvern hos behandlingsansvarleg: (lista er ikkje uttømmande):

- Uautoriserte personar får tilgang til personopplysningar. Det kan både vere personer utanfor eller innanfor organisasjonen.
- Medarbeidarar endrar eller slettar personopplysningar ved eit uhell.
- Innbrot på server, der uvedkommande har fått innsikt i personopplysningar
- Medarbeidarar gir vidare, bevisst eller ubevisst, personopplysningar om ein borgar/ brukar/ pasient til ein annan person eller kanskje til fleire andre uvedkommande
- Når it-system med personopplysningar ikkje er tilstrekkeleg sikra, slik at uvedkommande får tilgang til opplysningane (f.eks. hacking).
- Dersom den behandlingsansvarlege ulovleg eller som følgje av eit hendig uhell (til dømes brann eller overfløyming) i ein periode ikkje har tilgang til eller slettar/øydelegg personopplysningane

10.2 Mogelege konsekvensar av brot

I personvernforordninga er det nemnt nokre dømer på konsekvensar eit brot på personvernet kan ha. [1]

Eit brot kan, om det ikkje vert handtert på ein korrekt måte, påføre personar fysisk, materiell eller ikkje-materiell skade, slik som:

- tap av kontroll over deira personopplysningar eller avgrensing av deira rettar
- forskjellsbehandling
- identitetstjuveri eller svik
- finansielle tap
- uautorisert oppheving av pseudonymisering
- skade på omdøme
- tap av fortrulegheit av opplysningar som er omfatta av teieplikt
- andre betydelege økonomiske eller sosiale konsekvensar

10.3 Melding til Datatilsynet

Korleis sende melding til Datatilsynet?
Det skal nyttast eige skjema som er tilgjengeleg på Datatilsynet sine sider.

Kva brot på personopplysningssikkerheita skal meldast inn?
Som utgangspunkt skal alle brot på personvernet meldast til Datatilsynet.

Det er berre i dei tilfella det er usannsynleg at brotet inneber ein risiko for fysiske personar sine rettar eller fridom, at det **ikkje** skal meldast inn til Datatilsynet.
Ein risiko for fysiske personar sine rettar og fridom kan til dømes vere:

- diskriminering
- identitetstjuveri – eller svindel
- økonomisk tap
- skade på omdømme
- tap av fortruelege data underlagt tausheitsplikt
- ei vesentleg økonomisk eller sosial ulempe for den registrerte

[1] Personvernforordninga artikkel 4 nr. 12 og innleiinga til forordninga nr. 75, 85 og 86

Manglande etterleving av reglane for melding om brot på personvernet til Datatilsynet, kan resultere i at Datatilsynet til dømes uttalar kritikk eller utsteder eit påbod til den behandlingsansvarlege. Avhengig av omstende i kvart enkelt tilfelle kan det også verte snakk om sanksjonar i form av bøter - anten i kombinasjon med eller i staden for Datatilsynet sine pålegg.

Den behandlingsansvarlege skal straks etter å ha vorte kjend med brotet på personvernet, vurdere sannsynet for at brotet inneber ein risiko for personar sine rettar eller fridom. Det er snakk om ei konkret risikovurdering spesifikt i forhold til konsekvensane av brotet på personvernet.

Til forskjell frå ei vurdering av den potensielle risikoen som den behandlingsansvarlege til dømes skal ta i samband med ei konsekvensanalyse (DPIA), skal ei risikovurdering etter personvernforordninga sin artikkel 33 (og artikkel 34) ta utgangspunkt i risikoen for dei aktuelle personar som har oppstått som følgje av eit brot på personvernet.

Følgjande forhold bør alltid inngå i den konkrete vurderinga av risikoen for dei registrerte sine rettar eller fridom som følgje av eit brot på personvernet:

- Type brot, om det er skjedd tap av opplysningar, brot på fortrulegheita eller integriteten.
    - Omfanget til opplysningane
    - Risikoen for at den registrerte kan identifiserast
    - Konsekvensar brotet kan ha for den registrerte
- Om brotet omfattar særlege tilhøve ved den registrerte, som til dømes dersom det er snakk om barn eller særleg utsette.
- Talet på personar som er råka

Type brot
Kva konsekvensar eit brot på personvernet kan få for dei aktuelle personane er avhengig av kva type brot det er snakk om. Eit brot som gjer at personopplysningar ikkje lenger er tilgjengelege kan få heilt andre konsekvensar for den registrerte, enn dersom det til dømes er snakk om eit brot som resulterer i offentleggjering av personopplysningar.

Opplysningane sin art og omfang
I utgangspunktet vil opplysningane sin art ha innverknad på risikovurderinga. Dess meir sensitive opplysningar det er snakk om, dess større konsekvensar må eit sikkerheitsbrot antakast å få for dei aktuelle personane. Ei utilsikta offentleggjering av at ein person lir av ein spesiell sjukdom, vil kunne få større konsekvensar enn det å offentleggjere ein person si e-post adresse, eller CV.

Alle høve kring sikkerheitsbrotet skal takast i betraktning, derunder dei særlege omsyn som kan gjere seg gjeldande for dei som har fått sine personopplysningar eksponert. Offentleggjering av ei adresse vil normalt ikkje kunne forventast å få store konsekvensar, men dette kan vere annleis om adressa ein avslører tilhøyrer ein person som bur på hemmeleg adresse, på ein psykiatrisk institusjon eller liknande.

Omfanget av brotet, mengda av personopplysningar det gjeld, vil kunne få verknad for utfallet av risikovurderinga. T.d. vil eksponering av ei lita mengde sensitive personopplysningar kunne forårsake stor skade.

Den tidsmessige utstrekkinga av eit brot vil også kunne ha betyding, risikoen for dei registrerte vil vere større der opplysningane har vore tilgjengelege for uvedkomande i ei lengre periode. Men vi kan heller ikkje sjå bort frå at sjølv eit kortvarig brot kan få store konsekvensar.

Moglegheit for å identifisere personar
Ein faktor som spelar inn ved risikovurderinga er kor lett det vil vere å identifisere personen opplysningane er knytt til. Kryptering eller pseudonymisering vil gjere det vanskeleg å direkte identifisere ein person.
Definisjon på pseudonymisering: behandling av personopplysningar der dei ikkje lenger kan knyttast til eit bestemt register utan bruk av supplerande opplysningar, viss desse supplerande opplysningane oppbevarast separat og er underlagt tekniske og organisatoriske anstaltar, for å sikre at dei ikkje reknast til ein identifisert eller identifiserbar fysisk person.

Alvoret av konsekvensane for dei råka personane
Ved eit brot som vil gjere tilgjengeleg opplysningar om spesielt utsette eller sårbare personar, slik som barn, vil ein kunne vurdere brotet til å ha større skadeverknadar.

Dersom opplysningar hamnar i hendene på kriminelle som det kan forventast har vonde hensikter, vil dette ha stor betyding for risikovurderinga.

Viss opplysningane har hamna hos feil mottakar, som den behandlingsansvarlege har stor tillit til og forventar vil tilbakekalle eller destruere opplysningane etter instruks, vil dette kunne føre til at behandlingsansvarleg ser der ikkje er konsekvensar knytt til utleveringa og dermed ikkje treng melde dette til Datatilsynet.
Den behandlingsansvarlege bør då vere sikker i si sak, når mottakar si truverd har betydning for denne vurderinga. Den dataansvarlege bør samtidig, viss mogeleg, sikre seg dokumentasjon for at vedkommande ikkje lenger har rådigheit over opplysningane.

Konsekvensane ved eit sikkerheitsbrot vil som utgangspunkt vere større, viss dei strekk seg over lengre tid og er av ein meir permanent karakter, og dei ikkje utan vidare kan avgrensast av behandlingsansvarleg eller den registrerte sjølv.

Døme:
Tap av bankkort
Her vil konsekvensane truleg bli redusert ved å sperre kortet. Viss det derimot fører til spreiing av opplysningar som kan skade ein person sitt omdømme, vil dette kunne få langt større konsekvensar for vedkomande.

Særlege tilhøve ved den registrerte
Det kan få betyding for risikovurderinga dersom det er snakk om opplysningar om eit born eller ein annan sårbar person. Dette kan også vere tilfelle dersom det er snakk om til dømes offentleggjering av adresse- eller kontaktopplysningar til ein offentleg kjent person eller ein person som har hemmeleg adresse.

Talet på dei personane som er råka av brotet
Som utgangspunkt vil betydinga av eit brot på personvernet stige i takt med talet på personar som blir råka av brotet. Vi skal dermed ikkje sjå bort frå at brot på ein enkelt person eller få personar også vil kunne få alvorlege konsekvensar.

Tidsfrist for melding til Datatilsynet
Dersom det er sannsynleg at eit brot på personvernet er ein risiko for fysiske personar sine rettar eller fridom, skal den behandlingsansvarlege utan unødig forseinking og om mogleg seinast 72 timar etter at denne har blitt kjent med det, melde brotet til Datatilsynet.

Dersom det ikkje blir sendt melding til Datatilsynet innan 72 timar, må det følgje med ei grunngjeving for forseinkinga.

Plikta om å melde eit sikkerheitsbrot trer inn først frå det tidspunkt når behandlingsansvarleg «vart kjend med sikkerheitsbrotet». Dette bør føre til at den behandlingsansvarlege nøye vurderer om det faktisk har skjedd eit brot, og samtidig nytte høvet til å vurdere sikkerheita for behandlinga av personopplysningar.
I denne vurderinga kan det også leggast vekt på om dei opplysningane den behandlingsansvarlege er plikta melde Datatilsynet om, er gjort tilgjengeleg for behandlingsansvarleg.

Kven melder til Datatilsynet?
Som utgangspunkt er det den behandlingsansvarlege (kommunen) som melder eit brot på personvernet til Datatilsynet.

Den behandlingsansvarlege bør i samband med dette peike ut ein eller fleire medarbeidarar i organisasjonen som har fått delegert løyve til å melde brot på personvernet til Datatilsynet på vegne av den behandlingsansvarlege.

Ein databehandlar vil også kunne melde eit brot på personvernet til Datatilsynet på vegne av den behandlingsansvarlege. Dette er under føresetnad om at databehandlaren har fått delegert mynde til dette og at dette går fram av databehandlaravtalen som er inngått mellom partane.

Det overordna juridiske ansvaret for å melde eit brot på personvernet, og at dette skjer på riktig måte, ligg uansett hjå den behandlingsansvarlege.

Kva opplysningar har Datatilsynet bruk for?
Når behandlingsansvarleg melder eit brot på personvernet til Datatilsynet, skal meldinga som eit minimum:

- Skildre karakteren av brotet på personvernet. Kategoriane og det omtrentlege talet på dei aktuelle registrerte, samt tilsvarande om aktuelle registreringar av personopplysningar, om mogeleg.
- Angi namn på og kontaktopplysningar til Personvernombodet eller eit anna kontaktpunkt der det kan hentast inn fleire opplysningar.
- Skildre dei sannsynlege konsekvensane av brotet på personvernet.
- Skildre dei tiltaka som den behandlingsansvarlege har gjort eller foreslått å gjere for å handtere brotet på personvernet, og nødvendige tiltak for å avgrense moglege skadelege effektar.
- Andre opplysningar dersom det er formålstenleg.

Det at den behandlingsansvarlege ikkje er i stand til å gi alle opplysningane som minimum skal vere med i meldinga, innan tidsfristen på 72 timar, kan ikkje brukast som grunngjeving for å fråvike det overordna kravet om at brotet skal meldast til Datatilsynet innan 72 timar. Den

behandlingsansvarlege må i staden gi opplysningane trinnvis til Datatilsynet utan ytterlegare forseinkingar.

Situasjonar der det ikkje er naudsynt med melding til Datatilsynet
Eit brot på personvernet skal ikkje meldast til Datatilsynet dersom det er usannsynleg at brotet inneber ein risiko for fysiske personar sine rettar eller fridom.

Den behandlingsansvarlege skal ta alle tilhøva ved det aktuelle brotet i betraktning ved ei vurdering av risikoen for dei aktuelle personane sine rettar.

Den behandlingsansvarlege skal på den eine sida gjere dei sikkerheitstiltaka som kan redusere risikoen for dei aktuelle personane i betraktning, og på den andre sida dei tilhøva ved brotet som kan føre til auka risiko.

Det er det samla ***aktuelle*** risikobiletet som er avgjerande for om det skal skje ei melding om eit brot på personvernet til Datatilsynet.

Døme:
Ein tilsett i kommunen lastar ved ein feil opp ei fil på kommunen sine heimesider. Denne fila inneheld personnummer for fleire innbyggjerar i kommunen. Den tilsette blir raskt merksam på feilen og fjernar fila frå heimesida. IT-avdelinga i kommunen kan etter å ha undersøkt loggen til heimesida konstantere at det ikkje har vore besøkande på sida i den tida fila låg tilgjengeleg ute. Kommunen konkluderer samtidig, at der ikkje er noko som tyder på at fila har blitt kopiert av søkemaskiner som Google, Bing og likande. På bakgrunn av dette, vurderer kommunen at sannsynet for at fila har kome på avvege er så liten, at det ikkje trengs meldast til Datatilsynet.

10.4 Kva plikter har databehandlaren?

Databehandlaren har plikt til å underrette den behandlingsansvarlege om brotet utan unødig forseinking, dersom databehandlar blir merksam på at der har skjedd eit brot på personvernet.

Det er snakk om ei absolutt plikt som databehandlaren skal etterleve i alle tilfelle. Databehandlaren kan til dømes ikkje unnlate å underrette den behandlingsansvarlege om eit brot på personvernet med grunngjevinga at databehandlaren sjølv har vurdert at det er usannsynleg at brotet inneber ein risiko for fysiske personar sine rettar eller fridom. Det bør også skje underretting av den behandlingsansvarlege sjølv om databehandlaren trur at den behandlingsansvarlege allereie er kjent med brotet.

Databehandlaren skal straks underrette den behandlingsansvarlege

10.5 Underretning av den registrerte

Kva brot på personvernet krev underretning av den registrerte?
Dersom det er sannsynleg at brotet på personvernet vil medføre ein høg risiko for fysiske personar sine rettar eller fridom, skal den behandlingsansvarlege utan ugrunna opphald underrette den registrerte om brotet.

Dersom den behandlingsansvarlege ikkje gjer dette, har Datatilsynet ei moglegheit for å gå inn i saka, og krevje at den behandlingsansvarlege underrettar den registrerte.

Formålet med underretninga er blant anna å gje den registrerte moglegheit til å treffe dei naudsynte førehaldsreglane i tilfelle det er skjedd ei eksponering av vedkomande sine personopplysningar.

Eit brot på personvernet kan medføre store skadeverknadar for dei personane som er råka av brotet – som diskriminering, identitetstjuveri, eller svindel, økonomisk tap, skade på omdømme, tap av fortrulege data underlagt teieplikt eller ei kvar anna økonomisk eller sosial ulempe for den registrerte.

Personvernforordninga definerer ikkje omgrepet «høg risiko». Men ved ei vurdering av omfanget av risikoen, blir det lagt til grunn at dess meir alvorlege konsekvensar brotet kan medføre, dess større vil risikoen vere for dei råka personane. Tilsvarande vil eit større sannsyn for eit brot, innebere ein større risiko for dei registrerte.

Når den behandlingsansvarlege skal foreta ei risikovurdering, bør alle dei moglege konsekvensane og negative verknadane for den registrerte takast med i vurderinga. Dette omfattar såleis også dei «sekundære» konsekvensane for dei registrerte, som eit brot på personvernet kan medføre.

Den behandlingsansvarlege skal også, avhengig av sannsynet for negative verknadane, foreta underretning, uansett talet på dei råka som er registrert.

Døme:
Ei rekkje saker skal opprettast i det offentlege byggesaksarkivet i kommunen. Ved ein feil får saksbehandlar ikkje fjerna opplysningar om søkjar sitt personnummer til dei opplasta dokumenta. Det er snakk om 4 dokument frå 4 ulike byggesaker.
Kommunen bli først oppmerksam på feilen 2 månadar etter, ved at dei råka søkjarane har funne fram til dokumentet ved å søke på sitt personnummer via Google.
Kommunen sjekkar i samband med dette i gjennom dei andre sakene i byggesaksarkivet, og finn fram til dei 3 andre sakene, der same feil er skjedd.
Kommunen vil vere plikta å underrette dei råka personane om offentleggjeringa av deira personnummer. Dette på grunnlag av tida opplysningane har vore tilgjengelege via internett, samt omstenda med at eit personnummer vil kunne bli misbrukt til m. a identitetstjuveri.
Dei registrerte skal derfor ha høve til å ta dei rette forholdsreglane som følgje av offentleggjeringa.
Kommunen bør i samband med dette vidare rettleie dei registrerte om, kva forholdsreglar vedkommande kan ta med tanke på å redusere risikoen for misbruk av opplysningane.

Tidspunktet for underretninga
Den behandlingsansvarlege skal underrette den registrerte **utan unødig forseinking** etter at brotet på personvernet er påvist.

Underretninga er ikkje avhengig av tidspunktet for når meldinga av brotet til Datatilsynet skjer.

Kravet om underretning utan unødig forseinking, skal også sjåast i samanheng med formålet med underretninga. Den er i følgje personvernforordninga å gje den registrerte høve til å treffe dei naudsynte forholdsreglane.

Det går fram av forordninga at underretning til dei registrerte bør bli gitt så raskt som mogleg. Til dømes kan behovet for å avgrense ein direkte risiko for skade, krevje underretning av den registrerte, medan behovet for å gjennomføre passande tiltak mot vidare eller liknande brot på personvernet, kan vere ein grunn til ein lengre frist for underretning.

Døme: Det har skjedd eit brot på personvernet, og den registrerte si hemmelege fysiske adresse har blitt offentleggjort. Adressa er beskytta på grunn av at den registrerte kan risikere fysisk vold frå ein annan person. Her kan det vere avgjerande når den registrerte blir underretta om offentleggjeringa.

Døme: Mange brukar den same kombinasjonen av brukarnamn og passord til mange internettkontoar. Dersom nokon har fått tilgang til desse passorda i samband med eit brot på personvernet hjå ein dataansvarleg, vil ein tredjemann med stort sannsyn kunne få tilgang til andre kontoar tilhøyrande den gjeldande registrerte, slik som i nokre tilfelle e-postkonto. Konsekvensane for den registrerte kan i eit slikt tilfelle eventuelt avgrensast ved at dess raskare vedkomande vert underretta om brotet på personvernet, med ei klar anbefaling om å endre passord til alle kontoar som har eit liknande passord, dess mindre vil sannsynet for at nokon kan misbruke informasjonen vere.

Kva opplysningar skal vi melde?

Underretninga til den registrerte skal skildre karakteren av brotet på personvernet, og som eit minimum:

- Angi namn på og kontaktopplysningar til personvernombodet eller eit anna kontaktpunkt der ytterligare opplysningar kan innhentast.
- Skildre dei sannsynlege konsekvensane av brotet på personvernet.
- Skildre dei tiltaka den behandlingsansvarlege har treft eller foreslår for å handtere brotet på personvernet, også dersom det er relevant, førebyggande tiltak for å avgrense brotet sine moglege skadeverknadar.

Den behandlingsansvarlege kan avgjere å gje den registrerte ytterligare opplysningar om brotet enn det minimum som er oppgitt her, så lenge underretninga fortsatt er klar og lett å forstå.

Dersom det er relevant, bør den behandlingsansvarlege også gje den registrerte spesifikke råd om korleis den registrerte kan beskytte seg mot moglege negative konsekvensar av brotet.
Til dømes nullstilling eller endring av passord, dersom den registrerte sine passord har kome på avvege.

Underretninga av den registrerte skal bli gitt i eit klart og forståeleg språk og den behandlingsansvarlege bør derfor ta omsyn til mottakaren, og sikre seg at informasjonen er forståelig for vedkomande. Den behandlingsansvarlege bør i den samanheng ta omsyn til vedkomande sitt morsmål, språkkunnskap, alder osv.

Kravet må sjåast i samanheng med sjølve formålet med å underrette den registrerte om brotet på personvernet. Dersom underrettinga ikkje er tilstrekkelig klar og forståeleg for den registrerte, vil vedkomande ha vanskelig med å treffe dei naudsynte tiltaka for å redusere dei negative verknadane av brotet.

Den behandlingsansvarlege må i tillegg ikkje krevje nokon form for betaling for underrettinga eller dei tiltaka som den behandlingsansvarlege måtte ha treft for å beskytte den registrerte sine rettar og fridomar.

Korleis skal den registrerte bli underretta?
Korleis det er hensiktsmessig å underrette den registrerte, skal vurderast i forhold til det brotet som har skjedd på personvernet.

Den behandlingsansvarlege skal underrette den registrerte direkte, til dømes på e-post, brev, sms eller liknande. Ei underretting som avgrensar seg til eit presseoppslag eller eit oppslag på ei heimeside vil typisk ikkje vere nok. Informasjonen til den registrerte kan heller ikkje sendast til vedkomande saman med annan informasjon, som til dømes generelle oppdateringar, nyheitsbrev eller standardutsendingar frå den behandlingsansvarlege.

Det er anbefalt at den behandlingsansvarlege nyttar den metoden for underretting av dei registrerte som gir størst sjanse for at informasjonen om brotet på personvernet kjem fram til alle dei råka personane. Den behandlingsansvarlege kan vurdere å nytte fleire kommunikasjonsmetodar for å underrette dei registrerte.

Kven kan underrette dei registrerte?
Det er den behandlingsansvarlege som har ansvaret for å underrette dei råka personane om eit brot på personvernet.

Det er viktig i den samanheng å understreke at det overordna juridiske ansvaret, for at dei registrerte blir underretta, fortsatt blir hjå den behandlingsansvarlege, uansett om den behandlingsansvarlege har gitt mynde til databehandlaren.

Situasjonar der det ikkje er krav om underretning

- Dersom brotet ikkje vil vere ein høg risiko for den registrerte
- Det er gjennomført passande tekniske og organisatoriske tiltak
- Den høge risikoen for dei registrerte sannsynlegvis ikkje lenger er reell
- Krev ein uhøveleg innsats
- Utsetting av underretting i samsvar med nasjonal lovgjeving

Dersom det er lite truleg at brot fører til risiko for fysiske personar sine rettar og fridomar, treng ein ikkje melde frå til Datatilsynet. Med lite truleg meinast betydeleg mindre enn 50% sannsyn.

Alle vurderingar må dokumenterast og skal kunne etterprøvast av Datatilsynet.

Dersom brotet ikkje vil vere ein høg risiko
Det vil ikkje vere naudsynt å underrette den registrerte, dersom den behandlingsansvarlege etter ei vurdering av alle mogelege konsekvensar, kjem fram til at brotet ikkje har høg risiko for den registrerte sine rettar eller fridomar.

Døme: Ei kommune skal sende eit svar på e-post til ein innbyggjar som har søkt om løyve til å bygge eit påbygg på huset sitt. Ved ein feil kjem saksbehandlar hjå kommunen til å legge ved ei oversikt over alle dei eigedomane som har ei pågåande byggesak hjå kommunen. Av oversikta kjem det berre fram informasjon om søkarane sine namn, adresser og kommunen sitt saksnummer. Det er lista opp 15 eigedomar på oversikta. Kommunen blir dagen etter kontakta av innbyggjaren som gjer kommunen merksam på feilen. Det blir avtalt at innbyggjaren skal slette e-posten med det same, og at kommunen sender ein ny e-post med riktig innhald.

Underretning av dei registrerte vil ikkje vere naudsynt med omsyn til opplysningane sin karakter og talet på uberettiga mottakarar (1 person)

Bevisbyrda for vurderinga om at det ikkje vil vere ein høg risiko knytt til brotet på personvernet er den behandlingsansvarlege sitt ansvar. Den behandlingsansvarlege må til dømes i samband med ei sak hjå Datatilsynet, kunne angi kvifor den registrerte ikkje vart varsla.

Det er gjennomført passande tekniske og organisatoriske tiltak
Det vil ikkje vere naudsynt å underrette den registrerte dersom den behandlingsansvarlege har gjennomført passande tekniske og organisatoriske sikkerheitstiltak, og desse tiltaka er nytta på dei personopplysningane som brotet på personvernet gjeld. Dette gjeld spesielt tiltak som gjer personopplysningane uforståelege for alle som ikkje har autorisert tilgang, som til dømes kryptering.

Den høge risikoen for dei registrerte er sannsynlegvis ikkje lenger reell
Dersom den behandlingsansvarlege har innført tiltak som sikrar at den høge risikoen for dei registrerte sine rettar og fridom sannsynlegvis ikkje lenger er reell, vil det heller ikkje vere naudsynt å underrette dei registrerte.

Døme: *Eit it-system blir oppdatert og denne oppdateringa resulterer i utilsikta tilgang til sensitive personopplysningar utan pålogging. Dette vil gjere det mogleg for uvedkomande å få tilgang til personlege data frå Internett over ei kort periode.*
Databehandlar oppdagar etterpå at det har skjedd brot på personvernet og avbryter straks tilgang til uautoriserte brukarar slik at personopplysningane ikkje lenger er eksponerte.
I tillegg sett databehandlar i verk ei umiddelbar undersøking av detaljane i brotet på personvernet. Undersøkinga dokumenterer med sikkerheit kva tidsrom data har vore tilgjengeleg for uvedkomande. Undersøkinga dokumenterer også at det fins truverdige loggar, som ikkje kan omgåast og som har logga når personopplysningane vart vist i tidsrommet då personopplysningane var eksponerte. Det kan også dokumenterast på grunnlag av truverdig logginformasjon, at berre autoriserte brukarar faktisk har hatt tilgang personopplysningar i løpet av perioden då det var brot på personvernet.

Krev ein uhøveleg innsats
Den behandlingsansvarlege vil også kunne unnlate å underrette dei registrerte enkeltvis dersom det i det konkrete tilfellet vil krevje ein uhøveleg innsats.

Det skal skje ei avveging av på den eine sida verdien av ei slik underretting for den registrerte, og på den andre sida den arbeidsmengda den behandlingsansvarlege får med ei slik underretning.

I kva grad individuell melding til dei registrerte er uhøveleg vanskeleg eller kanskje til og med umogleg, skal avgjerast i kvar enkelt situasjon.

Underrettinga kan til dømes skje ved ei pressemelding.

***Døme**: Ei verksemd har mista tilgangen til alle kundeopplysningane i samband med at verksemda sin kundedatabase har blitt ramma av krypteringsvirus.* *Dersom ein gjer den avveginga at det vil krevje ein uhøveleg innsats av databehandlar å skulle underrette kvar enkelt registrert, må det i staden gjerast ei offentleg varsling der dei registrerte blir underretta på ein tilsvarande effektiv måte.*

10.6 Underretning etter krav frå Datatilsynet

Dersom den behandlingsansvarlege ikkje allereie har underretta den registrerte om brotet på personvernet, kan Datatilsynet etter å ha vurdert sannsynet for at brotet på personvernet vil vere ein høg risiko, krevje at den behandlingsansvarlege gjer det.
Moglegheita Datatilsynet har til å krevje underretting, er uavhengig av om den behandlingsansvarlege er einig med Datatilsynet.

Situasjonen kan til dømes oppstå i samband med ei melding av eit brot på personvernet til Datatilsynet, der den behandlingsansvarlege grunngjev sitt val om å ikkje underrette den registrerte. Dersom Datatilsynet meiner at der ikkje er tilstrekkelige haldepunkt for den manglande underrettinga, vil tilsynet pålegge den behandlingsansvarlege at dei skal underrette den registrerte.

Datatilsynet kan også komme fram til at den behandlingsansvarlege ikkje treng å underrette den registrerte.

Den behandlingsansvarlege kan bli bøtelagt som følgje av manglande etterleving av underretting av dei registrerte.

10.7 Ansvarlegheit og intern dokumentasjon

Den behandlingsansvarleg skal dokumentere alle brot på personvernet, også dei faktiske omstenda rundt brotet, konsekvens og tiltak som er gjort.

Det er i det høve utan betyding om brotet er av ein slik karakter at den behandlingsansvarlege er forplikta til å melde til Datatilsynet eller ikkje. **Det skal altså dokumenterast også i dei tilfella der den behandlingsansvarlege har vurdert at brotet ikkje vert meldt inn.**

Formålet med dokumentasjonsplikta er å sette Datatilsynet i stand til å kontrollere, om plikta i personvernforordninga, for å melde inn visse brot på personvern, er overhalde. Plikta heng likevel også saman med forordninga sitt prinsipp om ansvarlegheit (”accountability ”).

Den behandlingsansvarlege har plikt til å utlevere dokumentasjon til Datatilsynet, om dei ber om dette.

Dokumentasjonen skal innehalde informasjon om brotet, også dei faktiske omstenda rundt brotet, konsekvens og tiltak som er gjort for å utbetre dette[2]. Krava til dokumentasjon skal innehalde:

- Dato og tidspunkt for brotet
- Kva skjedde i samband med brotet?

[2] Artikkel 33 pkt. 5

- Kva er årsaken til brotet?
- Kva (typar) personopplysningar er omfatta av brotet?
- Kva konsekvensar har brotet for den/dei personen(-ane) dette gjeld?
- Kva tiltak er sett inn?
- Skal det meldast til Datatilsynet eller ikkje?

Dokumentasjonen – i forhold til avgjerda om ikkje å melde til Datatilsynet – skal omfatte ei nærare utgreiing om kvifor den behandlingsansvarlege meiner at brotet sannsynlegvis ikkje vil medføre risiko for dei fysiske personane sine rettar og fridom.

Tilsvarande dokumentasjon må også ligge føre i forhold til vurdering om å underrette den registrerte og at vilkår for ikkje å underrette er oppfylt.

Dersom den behandlingsansvarlege melder inn eit brot på personvern til Datatilsynet, etter utgått frist på 72 timer, skal den innehalde grunngjeving for forseinkinga.
Dokumentasjon knytt til saka skal ligge ved.

Eksempel på internt dokumentasjonsregister:

Brot på personvern hjå – *[SET INN NAMN PÅ BEHANDLINGSANSVARLEG]*	**Skildring av brotet**
1. Dato og tidspunkt for brotet	
2. Kva skjedde i samband med brotet?	
3. Kva er årsaken til brotet?	
4. Kva (typar) personopplysningar er omfatta av brotet?	
5. Kva konsekvensar har brotet for den/dei personen(-ane) dette gjeld?	
6. Kva tiltak er sett inn?	
7. Er brotet meldt til Datatilsynet (om ja, kva tid)?:	
8. Dersom nei, grunngjeving for ikkje å melde til Datatilsynet?:	
9. Er den registrerte underretta (om ja, kva tid)?	
10. Dersom nei, grunngjeving for ikkje å ha underretta den registrerte	

10.8 Implementering i organisasjonen

Det er heilt avgjerande at den behandlingsansvarlege (og databehandlar) utarbeidar prosedyre for handtering av sikkerheitshendingar i organisasjonen, for å kunne sikre ei effektiv etterleving av plikta om å melde brot på personvernet til Datatilsynet, og til å underrette den registrerte.

Den behandlingsansvarlege bør i den samanheng ta med forholdet til eventuelle databehandlar og deira underleverandørar, slik at prosedyrane også tek høgde for personvernet med dei.

Den behandlingsansvarlege (og databehandlar) bør vidare tenke gjennom kva tekniske og organisatoriske tiltak som kan innførast i organisasjonen, for å sikre at brot på personvernet vert oppdaga.

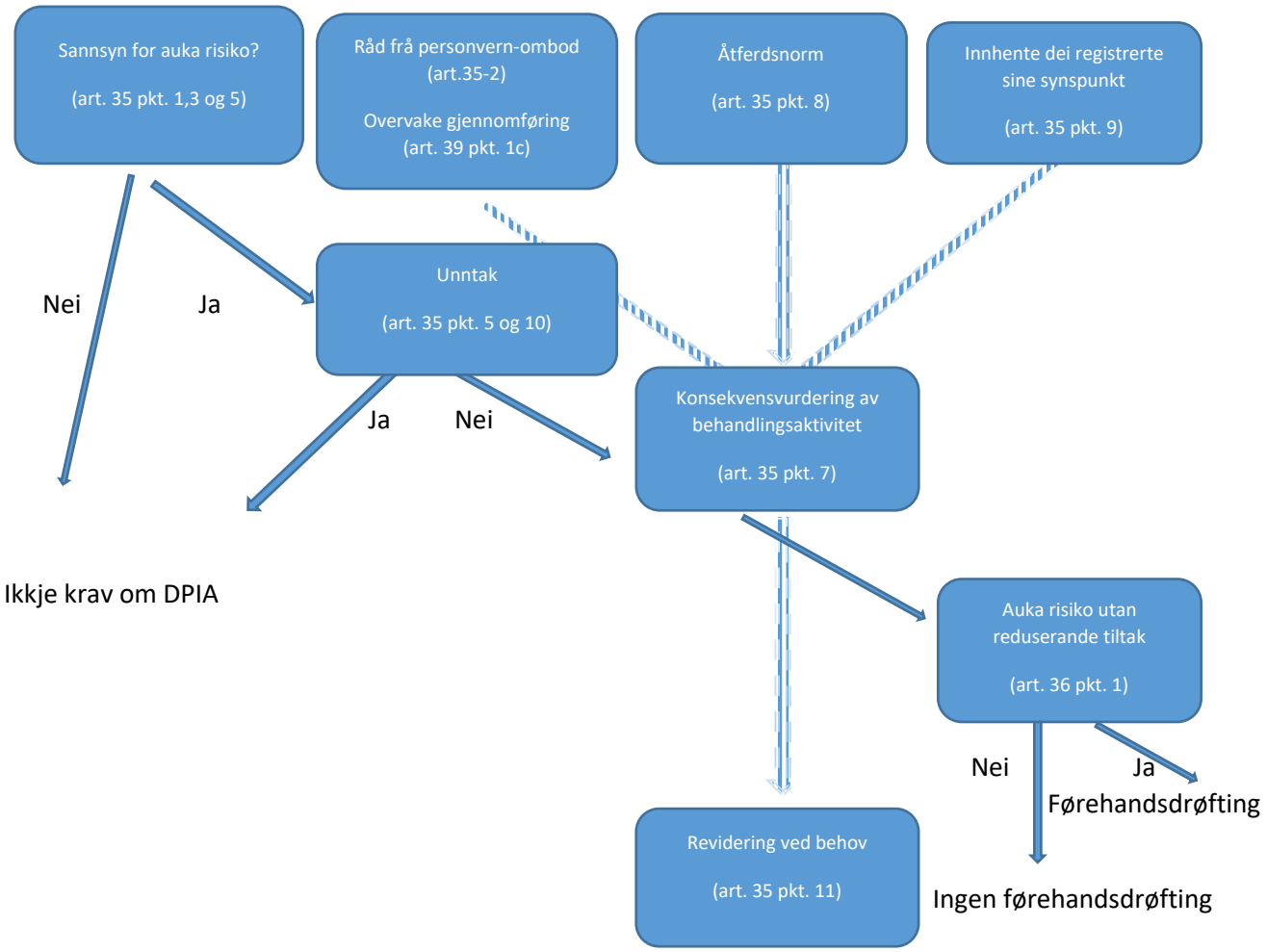
11 Vurdering av personvernkonsekvens – DPIA

Vurdering av personvernkonsekvens (heretter kalla DPIA) er ein systematisk prosess, som identifiserer og evaluerer – frå alle interessentar sin synsvinkel – potensielle personvernkonsekvensar i eit prosjekt, initiativ, foreslått system eller prosess. Dette inkluderer vurderingar om korleis unngå truslar mot personvernet, eller tiltak som må setjast i verk for å avverje truslar mot personvernet. DPIA skal ha et særlig fokus på risiko for den registrerte.

Ein "risiko" er eit scenario som beskriv ei hending og konsekvensen av den, som vurderast i forhold til alvor og sannsyn. På den andre side kan "risikostyring" definerast som samordna aktivitetar knytt til styring og kontroll av ein organisasjon med omsyn til risiko.

Om ei behandling med stort sannsyn vil innebere høg risiko for fysiske personar sine rettar og fridom, skal det gjennomførast DPIA.

Prinsipp i samband med DPIA



Sannsyn for auka risiko? (art . 35 – 1,3 og 5)
Som behandlingsansvarleg skal vi kartleggepersonvernkonsekvensar for særleg å vurdere risikoen sitt opphav, art, særpreg og alvorsgrad. For å bestemme eigna tiltak, bør det takast omsyn til utfallet av vurderinga

Dersom konsekvensvurderinga viser at behandlingsaktivitetane inneber ein høg risiko for fysiske personar sine rettar og fridom, som den behandlingsansvarlege ikkje kan avgrense ved å treffe eigna tiltak (der det vert teke omsyn til tilgjengeleg teknologi og gjennomføringskostnadar), skal vi rådføre oss med tilsynsmynde før behandlinga tek til.

Råd frå personvernombod og overvake gjennomføring (art.35-2) og (art. 39 – 1c)
Den behandlingsansvarlege må rådføre seg med **personvernombodet.** Personvernombodet sitt råd saman med avgjerslene den behandlingsansvarlege tek, skal dokumenterast i vurderinga.

Personvernombodet skal også kontrollere gjennomføringa av DPIA.

Åtferdsnorm – bransjenorm (art. 35-8)
Ei bransjenorm er eit regelsett for ein spesifikk bransje. Den skal gi konkrete reglar og retningsliner for korleis verksemdene skal innrette seg for å etterleve krava i personvernforordninga. Ei bransjenorm er utvikla av bransjen sjølv. Det er Datatilsynet som godkjenner den.

Eit døme på bransjenorm er «Norm for informasjonssikkerhet helse og omsorgstjenesten (Normen)».

Innhente dei registrerte sine synspunkt (art. 35-9)
Dersom det er relevant skal behandlingsansvarleg hente inn opplysningar frå den registrerte eller den som representerer denne. (Døme: Verje, pårørande, advokat, interesseorganisasjon)

Dettefor å sikre at den registrerte sine ev. innvendingar og bekymringar vert vurdert av behandlingsansvarlege. På denne måten får vi betre innsikt i den registrerte sin ståstad, og kan skape auka tillit til verksemda og måten vi behandlar personopplysningar på.

Unntak (art. 35-5 og 10)
Datatilsynet **er pålagt å** publisere liste over behandlingsaktivitetar som krev at vi vurderer personvernkonsekvensar.

Datatilsynet *kan* publisere liste over behandlingsaktivitetar som *ikkje* krev at vi vurderer personvernkonsekvensar.

Merk at Justisdepartementet har skrevet følgende i proposisjon 56 LS(2017-2018), kapittel 16.5.5:

> *«Etter departementets vurdering er unntaket fra plikten til vurdering av personvernkonsekvenser i forordningen artikkel 35 nr. 10 så snevert at det ikke synes nødvendig på nåværende tidspunkt å fastsette noen nasjonale unntak fra unntaket. Unntaket kommer bare til anvendelse når det supplerende rettsgrunnlaget for behandlingen inneholder en spesifikk regulering av de ulike behandlingsaktivitetene, noe som sjelden er tilfelle. Hvis behandlingsaktivitetene først er spesifikt regulert i lov eller forskrift, og personvernkonsekvensene allerede er vurdert i den forbindelse, kan departementet ikke se at en vurdering av personvernkonsekvenser vil ha en så stor tilleggsverdi at det er nødvendig å pålegge dette også i disse tilfellene.*
>
> *At unntaket fører til grensedragningsspørsmål, er etter departementets oppfatning ikke et tilstrekkelig tungtveiende hensyn til at det er nødvendig å pålegge en plikt til vurdering av personvernkonsekvenser. Risikoen for misforståelser av rekkevidden av unntaket kan*

reduseres med informasjon og veiledning. Departementet foreslår ingen utvidet plikt til forhåndsdrøfting med tilsynsmyndigheten etter artikkel 36 nr. 5. Det foreslås imidlertid en forskriftshjemmel som åpner for slike bestemmelser, se lovforslaget § 14.»

I datatilsynet sin rettleiar finn vi fire punkt der DPIA ikkje er nødvendig:

- dersom behandlinga ikkje medfører høg risiko
- dersom det er vurdering av liknande behandling tidlegare (då kan vurderinga brukast opp att)
- dersom behandlinga har vore underlagt konsesjonsplikt før mai 2018 og ikkje har endra seg
- dersom lovverk gir grunnlag for å sjå vekk frå det

Konsekvensvurdering av behandlingsaktivitet (art. 35-7)
Innhaldet i konsekvensvurderinga skal som eit minimum innehalde:

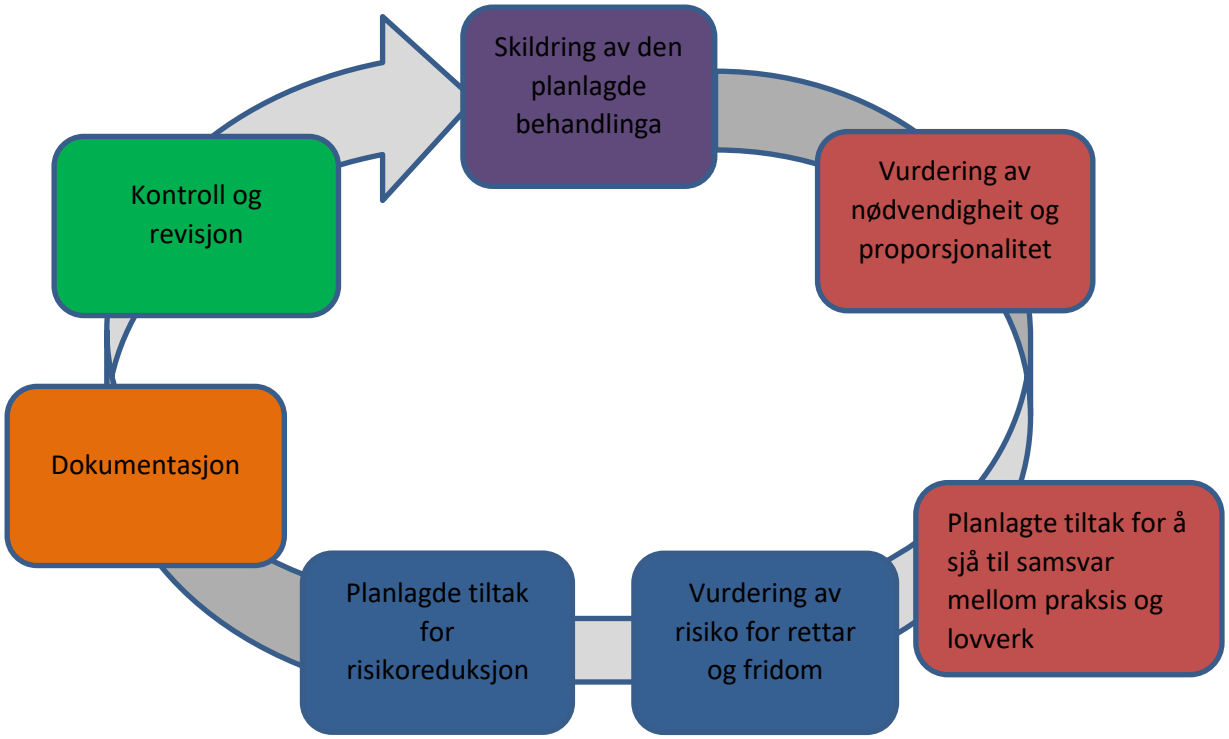
- ei systematisk skildring av dei planlagde behandlingsaktivitetane og formåla med behandlinga
- ei vurdering av om behandlingsaktivitetane er nødvendige og står i rimeleg forhold til formåla
- ei vurdering av risiko for dei registrerte sine rettar og fridom og
- dei planlagde tiltaka for å handtere risiko

Auka risiko utan reduserande tiltak (art. 36-1)
Dersom reduserande tiltak likevel ikkje reduserer risikoen til akseptabelt nivå, krev tilsynsmynde førehandsdrøfting. Føresetnaden er at behandlinga framleis har høg risiko ved at den kan ha høg verknad, innblanding eller krenking av personvernet eller dei registrerte sine rettar og fridom, og at denne risikoen ikkje kan reduserast.

Gjennomgang av vurdering gjort av behandlingsansvarleg (art. 35-11)

Gjennomføring av DPIA er ein kontinuerleg prosess.

11.1 Prosess for gjennomføring av DPIA



1. Når er det ein høg risiko?

Personvernkonsekvensutredning (DPIA) skal gjennomførast når det er «høg risiko» for den registrerte sine rettar og fridom. I denne vurderinga er det fleire moment det kan leggast vekt på.

For det fyrste skal det alltid utførast ein DPIA når den planlagte behandlinga står på **Datatilsynet si liste**. *(Dette inkluderer til dømes bruk av velferdsteknologi, evaluering av læring, trivsel, mestring i bhg og skule, kameraovervåkning, lokasjonsdata med meir).*

Vidare skal det utførast ein DPIA når det er ein høg risiko for den registrerte sine rettar og fridom. Nedanfor er det lista opp moment i denne vurderinga.

Lovteksten gir for det første tre forhold som tilseier høg risiko og at det difor må utførast ei konsekvensutgreiing:

- systematisk og omfattande vurdering av personlege forhold når opplysningane vert nytta til automatiserte avgjersle
- behandling av sensitive personopplysningar i stort omfang
- systematisk overvaking av offentleg område i stort omfang

Vidare vil det dersom man svarar ja på 2 eller fleire av følgande spørsmål sannsynligvis vere nødvendig å utføre ei personvernkonsekvensvurdering:

1. Er behandlinga ei evaluering eller poengvurdering?
2. Omfatter den automatiserte avgjersler?
3. Inneber den systematisk overvakning?
4. Involverer den sensitive personopplysningar?

5. Dreiar det seg om ei behandling i stor skala?
6. Vil to eller fleire datasett samanstillast?
7. Omfattar den personopplysningar om registrerte med særskilt beskyttelsesbehov? (f.eks. barn, eldre, psykisk syke)
8. Vert det tatt i bruk ny teknologi eller nyttast eksisterande teknologi til nye formål?
9. Vil konteksten for behandlinga avgrense moglegheita dei registrerte har til å utøve sine rettar?

I tillegg kan følgande moment vurderast for å sjå om risikoen er høg:

Art
Behandlinga sin art tilseier at risikoen er høg. Relevante vurderingsmoment under behandlinga sin art er om behandlinga gjer det vanskeleg for den registrerte å utøve sine rettar, om behandlinga er uforutsigbar og om det er usikkerheit om dei grunnleggande prinsippa for behandling av personopplysningar vert tekne i vare., jf. Artikkel 5. Dersom behandlinga skjer kontinuerleg og systematisk kan det også tilseie at det er ein høg risiko

Omfang
Omfang av behandlinga kan tilseie at risikoen er høg. Det kan til dømes vere når det vert behandla **store mengder** personopplysningar som kan **påverke mange.**

- tal på involverte registrerte
- volum av innsamla data
- lagringstid
- geografisk omfang

Formål
Dersom opplysningane skal nyttast på ein slik måte at den grip inn i den private sfære kan det tilseie at risikoen er høg slik som t.d.

- kontrollformål
- avgjersle om einskildpersonar basert på systematisk og omfattande analyse av personlege forhold
- der målet er å ta avgjersle som har betyding for den registrerte

Samanheng (kontekst)
Samanhengar som tilseier at risikoen kan vere høg, er situasjonar der den registrerte har ei klar forventning om personvern knytt til behandlinga slik som:

- konfidensialitet (helse-, velferd og arbeidsforhold)
- privatliv (i heimen og på rekreasjon)
- der opplysningar er innhenta frå ulike datasett, innsamla til ulike formål og til ulike behandlingsansvarlege

Det må gjerast ei samla vurdering av momenta ovanfor for å vurdere om det føreligg ein høg risiko. Vurderingane bør dokumenterast i ei Risiko-analyse som kan nyttast som utgangspunkt for ei personvernkonsekvensutredning. I tvilstilfelle bør det gjennomførast ei personvernkonsekvensutredning. Dokumenter eventuelt kvifor ei personvernkonsekvensutredning ikkje er gjennomført.

2. Gjennomføringa av DPIA

Når det er vurdert at behandlingsaktiviteten inneber ein høg risiko, skal følgande moment vurderast og dokumenterast:

- Systematisk skildring av behandlinga, formål, og eventuelt kva berettiga interesse den tek i vare
- Vurdering av nødvendigheit og samhøve (forholdsmessighet), sett opp mot formålet
- Vurdering av risikoen for rettar og fridom til registrerte
- Tiltak som skal settast i verk for å redusere risikoen

Nedanfor følgjer ein mal som kan nyttast som utgangspunkt for gjennomføringa. I tillegg anbefalar vi å lese Datatilsynets veileder for vurdering av personvernkonsekvenser.

Mal for gjennomføring av DPIA

1. Skildring av den planlagde behandlinga

I innleiinga skildrar du kva behandling som skal starte, og kva system som skal nyttast for behandlinga. Det må presiserast om det er ei ny behandling, eller ei endring av eksisterande behandling.

2. Systematisk skildring
Behandlinga sin art

- Korleis skal opplysningane samlast inn?
- Korleis skal opplysningane lagrast?
- Kva er kjelda til opplysningane (den registrerte sjølv, innhenting frå andre?
- Skal opplysningane delast med andre?

Behandlinga sin omfang

- Kva opplysningar skal samlast inn?
- Skal særlege kategoriar av personopplysningar behandlast?
- Kor ofte skal innsamlinga skje?
- Lagringstida for opplysningane
- Kven vil det samlast inn opplysningar om?
- Kva geografisk område for behandling av personopplysningane? (lokalt, regionalt, nasjonalt eller internasjonalt?)

Formål

- Kva ynskjer kommunen å oppnå med behandlinga?
- Beskriv alle formål med dei ulike behandlingane (til dømes formålet med innsamling, formålet med oppbevaring, formålet med å dele opplysningane)
- Vil det vere kontrollformål?
- Kva er den ønska innverknaden på dei registrerte?
- Skal opplysningane vidarebehandlast til andre formål?

Berettiga interesse: Dersom behandlinga er *basert på art. 6 bokstav f) berettiga interesse, beskriv interesseavveininga som er gjort. [punktet slettast dersom ikkje relevant].*

ant].

Sammenheng behandlinga utførast i

- Kva relasjon har den behandlingsansvarlege med dei registrerte? (definer *maktforhold*)
- Kva kontroll vil den registrerte ha over opplysningane?
- Korleis vil den registrerte oppfatte behandlinga? Er det sannsynleg at vedkomande vil verte overraska eller ha eit negativt syn?
- Er det opplysningar om sårbare registrerte? (*ansatte, barn, psykisk sjuke, pasientar, asylsøkearar m.m*.)
- Vil den registrerte forvente at opplysningane vert behandla konfidensielt/ikkje delast med andre? (til dømes *helseopplysningar, kommunikasjon, arbeidsforhold, lokasjon*?)
- Vert det nytta teknologi som det tidligare har vore bekymringar om?
- Definer relevant status på den teknologiske utviklinga på feltet.
- Er Behandlingsansvarleg knytt til ein bransjenorm? (Til dømes *Norm for informasjonssikkerheit i helsetenesta*)

Kjelder, mottakar og informasjonssikkerheit

- Er det fleire Behandlingsansvarlege?
- Kvenskal få/ha tilgang til opplysningane? (tilsette, databehandlarar, eksterne verksemder?)
- Kva opplysningar vert delt eksternt? Kva er formål og rettsleg grunnlag for å dele opplysningane eksternt? (kan vere til andre offentlege myndigheiter)
- Skriv kva forhåndsreglar som vert tekne for å sikre personopplysningane (til dømes fysisk sikring, passordbeskytting tilgangskontroll, bransjenorm, andre tiltak)
-

Forholdet til databehandlar (*det kan vere nyttig å finne fram databehandlaravtale i denne delen)*

- Kva databehandlarar nyttast? (*også underleverandørar reknast som databehandlarar*)
- Kva opplysningar har databehandlar tilgang til?
- Er databehandlar eller underleverandør utanfor EU/EØS? Kva er det rettslege grunnlaget for overføringa?
- Er det inngått databehandlaravtale?
- Regulerar databehandlaravtalen alt som er nødvendig etter artikkel 28?

3. Synspunkt

- Kva er dei registrerte sitt syn på Behandlinga? (kan innhentast ved spørjeundersøking, spørsmål til tillitsvalgde e.l.) Eventuelt – kvifor er ikkje dei registrerte spurde?
- kva er personvernombodet sitt syn på behandlinga?

4. Vurdering av nødvendighet og proporsjonalitet

- Kva er behandlingsgrunnlaget?
- Er alle personopplysningane nødvendige for å oppnå formålet med behandlinga? (begrunn relevans og nødvendigheit for kvar av de ulike kategoriane av personopplysningar)
- Korleis hindre at personopplysningane nyttast til andre formål enn opprinneleg tenkt?
- Korleis sikrast det at opplysningane er korrekte?
- Korleis sikrast det at opplysningane er oppdaterte?

- Korleis sikrast det at opplysningane ikkje lagrast lengre enn nødvendig? Skild når sletting skjer.

Den registrerte sine rettar

- Kva informasjon får dei registrerte om behandlinga? Oppfyller informasjonen krava i art. 14-16?
- Korleis vert rettentil sletting og retting teken i vare?
- Korleis vert retten til dataportabilitet teken i vare?
- Korleis vert retten til avgrensing av behandlinga teken i vare?

Den registrerte sine fridomar

Vurder korleis dei registrerte sine fridomar i høve til Den europeiske menneskerettskonvensjonen (EMK) er teke omsyn til:

- Retten til privatliv og kommunikasjonsvern
- Retten til å ikkje bli diskriminert
- Tanke-, tru- og religionsfridom
- Ytrings-, og informasjonsfridom

5. Vurdering av risiko og planlagde tiltak for å handtere risiko

Her skal det lagast ei oversikt over risiko for den registrerte sine rettar og fridomar, samt kva tiltak som er gjorde for å sikre desse.

Planlagde tiltak for å sikre samsvar mellom praksis og lovverk
Det skal vere samsvar mellom praksis og lovverk. Tiltak som vert sett i verk skal sjå til dette.

Planlagde tiltak for risikoreduksjon
Her må tiltak som er sett i verk for å oppfylle de registrerte sine rettar **utover** minimumskrava, når behandlinga utgjer ein særskilt **risiko** for dei registrerte (basert på art, omfang, formål og samanheng) skildrast.

6. Godkjenning og dokumentasjon

Dersom tiltak som er sett i verk reduserar risikoen til et akseptabelt nivå, kan personvernkonsekvensutgreiinga godkjennast og behandlinga kan byrje. Dersom risikoen fortsatt er til stades må det gjennomførast ei førehandsdrøfting med datatilsynet.

Dokumentasjon
Dette skal dokumenterast:

- **Systematisk skildring av behandlinga**
- Konsekvensvurdering av behandlingsaktivitet
- Råd frå personvernombod og overvaking av gjennomføring
- Innhente dei registrerte sine synspunkt
- Grunngjeving dersom det ikkje vert innhenta synspunkt frå dei registrerte
- Tiltak som vert sett i verk

Kontroll og revisjon
Personvernombodet skal kontrollere at konsekvensvurderinga er gjort og eventuelt om den er utført korrekt.

Behandlingsansvarleg er ansvarleg for gjennomføring og for revisjon av vurderinga.

12 Personvernerklæring

Når nyttar vi personvernerklæring?

Ei personvernerklæring fortel korleis ein samlar inn og brukar personopplysningar.

For å få ei brukarvennleg personvernerklæring, er det mogleg å lage ein kortversjon med lenke til lengre og fullstendig tekst.

Når skal vi ha ei personvernerklæring?

- Når vi samlar inn personopplysningar om nokon
- Dersom vi får personopplysningar frå andre kjelder enn personen sjølv, skal dei få ei personvernerklæring;
    - Innan rimeleg tid etter innsamlinga av data, og seinast innan ein månad
    - Seinast ved første kommunikasjon vi har med dei, dersom vi samlar inn data gjennom kommunikasjonen med dei
    - Dersom vi planlegg å overføre data til ein tredjepart, seinast når data er overført

Kva typar personvernerklæring treng vi?

- For tilsette
- For søkjarar
- For brukarar/kundar
- Ei personvernerklæring for Internett
- Ei personvernerklæring for Intranett

Korleis skal vi utforme ei personvernerklæring?

- Kortfatta og presis informasjon
- Innehalde all nødvendig informasjon
- Forståeleg
- Lett tilgjengeleg form
- Bruke klårt og tydeleg språk

Forandringar i informasjonen

- Personvernerklæringa skal jamleg reviderast, og informasjonen skal oppdaterast ved endringar
- Dersom vi planlegg å bruke personopplysningane til eit nytt formål, skal vi oppdatere personvernerklæringa og varsle om endringane på førehand

12.1 Sjekkliste – kva skal vere med i ei personvernerklæring

Dette skal vere med	**Set kryss**
Namn og kontaktinformasjon til den behandlingsansvarlege (kommunen)	
Namn og kontaktinformasjon til dei som representerer kommunen (dersom relevant)	
Namn og kontaktinformasjon til kommunen sitt personvernombod	
Formålet med behandlinga av personopplysningane (kvifor opplysningane blir behandla)	
Det rettslege grunnlaget (lenke til protokoll over behandling av personopplysningar)	
Dei legitime interessene for behandling av personopplysningane (dersom dette er relevant)	
Kva type personopplysningar som vert samla inn (dersom personopplysningane ikkje er henta inn frå personen dei gjeld)	
Detaljar rundt overføring av personopplysningar til land utanfor EU/EØS (om aktuelt)	
Mottakarar eller kategoriar av mottakarar av personopplysningane	
Oppbevaringsperioden for opplysningane	
Rettane den enkelte har i samband med behandling av personopplysningane	
Retten til å trekke samtykket (dersom det er relevant)	
Retten til å klage til ei tilsynsmyndigheit	
Kvar personopplysningane er/blir henta frå (dersom dei ikkje er/blir henta frå den det gjeld)	
Detaljar om i kva grad den enkelte har ei lovfesta eller kontraktfesta plikt til å gi frå seg personopplysningar (dersom det er relevant, og dersom personopplysningane blir henta direkte frå den registrerte) / Er det frivillig å gi frå seg opplysningane? (Dersom opplysningane blir henta direkte frå den registrerte, må kommunen opplyse om det er frivillig for vedkomande å gje frå seg personopplysningar)	
Detaljar om automatiserte vedtaksprosessar (dersom det er relevant)	
Rett til dataportabilitet (dersom det er relevant)	
Korleis opplysningane vert sletta og arkivert. skildre kva rutinar kommunen har for å slette og arkivere personopplysningane	
Korleis opplysningane vert sikra. skildre kva sikringstiltak kommunen har ved behandling av personopplysningane, så langt denne informasjonen ikkje svekkjer sikkerheita	

13 Stillingsomtale og føresetnadar for personvernombod

Det skal peikast ut personvernombod når behandlinga vert gjort av offentleg mynde eller organ. Kommunane har offentleg mynde og skal difor ha personvernombod, som er gjort offentleg og meldt inn til Datatilsynet, jf. GRDP art 37.

Personvernombodet skal:

- På rett måte og til rett tid involverast av behandlingsansvarleg i alle spørsmål som gjeld personvern, jf. art 38
- Rapportere til høgste leiarnivå (rådmann), jf. art 38
- Ha naudsynte ressursar til rådvelde, ha tilgang til personopplysningar og behandlingsaktivitetar, jf. art 38
- Moglegheiter for å oppretthalde djupnekunnskap, jf. art 38
- Overhalde teieplikta, jf. art 38

Personvernombod skal *ikkje*:

- Ta i mot instruksjon i utføringa av oppgåvene, jf. art 38
- Straffast eller verte sagt opp som fylgje av utføring av rolla som personvernombod, jf. art 38

Ansvar og oppgåver:

- Vere kontaktperson for innbyggjarane i alle typar personvernspørsmål, jf. art 38
- Gje råd og rettleiing til behandlingsansvarleg og tilsette om personvern, jf. art 39
- Gje råd om vurderingar av personvernkonsekvensar og kontrollere gjennomføring av denne, jf. art 39
- Kontrollere at retningsliner og rutinar innan personvernområdet vert fylgd opp internt og vert haldne, jf. art 39
- Kontrollere det haldningsskapande arbeidet og revisjon, jf. art 39
- Samarbeide med Datatilsynet og fungere som kontaktperson for tilsynsmynde, jf. art 39

14 Nyttige Lenker

Generelt om GDPR:

Datatilsynet i Noreg

Datatilsynet i Danmark

Lenker knytt til vurdering av personvernkonsekvensar

Datatilsynet sin rettleiar for vurdering av personvernkonsekvensar

Retningslinjer DPIA artikkel 29 gruppa

Datatilsynet si sjekkliste for gjennomføring av vurdering av personvernkonsekvensar

15 Vedlegg

15.1 Malar - Rutine for opplysningsplikt

15.1.1 Mal - Underretning om innsamling av personopplysningar

Vi sender deg dette brevet for å orientere om at vi har fått personopplysningar om deg.

Etter personopplysningslova og personvernforordninga[3] sin art. 14, pliktar vi å gje deg ei rekkje opplysningar når vi innhentar eller får opplysningar om deg frå andre.

Dei opplysningane vi skal gje deg er følgande:

- Vi er den behandlingsansvarlege – korleis kontaktar du oss?
- Kontaktopplysningar på personvernombodet
- Formåla og det rettslege grunnlaget for behandlinga av dine personopplysningar
- Kategoriar av personopplysningar
- Mottakarar eller kategoriar av mottakarar
- Overføring av opplysningar til mottakarar i land utanfor EU, derunder internasjonale organisasjonar
- Kvar personopplysningane vi har innhenta om deg kjem ifrå
- Oppbevaring av dine personopplysningar
- Automatiske avgjersler, derunder profilering
- Retten din til å trekkje ditt samtykke attende
- Dine rettar
- Klage til Datatilsynet

I vedlagte bilag 1 er dette nærare utdjupa.

Vi sender dette brevet berre som ei orientering, og saka gjev ikkje umiddelbart høve til saksbehandling overfor deg.

Har du spørsmål, er du velkomen til å kontakte oss.
Våre kontaktopplysningar går fram av bilag 1.

Med venleg helsing

[Set inn namn på den behandlingsansvarlege]

[3] Europa-Parlamentets og Rådets forordning (EU) 2016/679 frå 27. april 2016 om vern av fysiske personar i samband med behandling av personopplysningar, og om fri utveksling av slike opplysningar og om oppheving av direktiv 95/46/EF. Av artikkel 14 (1) går det fram at den behandlingsansvarlege skal gje den registrerte ei rekkje opplysningar, når personopplysningar ikkje er innsamla frå den registrerte.

15.1.2 Bilag 1: Mal - Underretning om innsamling av personopplysningar

[MAL – TA BERRE MED DET SOM ER NAUDSYNT FOR DI BEHANDLING OG FJERN ALL HJELPETEKST!]

Opplysningar om *[Set inn namn]* kommune si behandling av dine personopplysningar

*[Set inn namn]*kommune ved *[Set inn namn/avdeling/telefon/e-post]* er behandlingsansvarleg for behandlinga av dei personopplysningane vi har motteke om deg.

Dersom du har spørsmål knytt til vår behandling av dine personopplysningar kan du også kontakte vårt personvernombod på:

E-post: *[Set inn e-post]*

Telefon: *[Set inn telefonnummer]*

Postadresse: *[Set inn adresse]*

1. **Formålet med og det rettslege grunnlaget for behandlinga av dine personopplysningar**

Vi behandlar dine personopplysningar for følgjande formål:

[Skildre formålet med denne behandlinga]

Det rettslege grunnlaget for vår behandling av dine personopplysningar følgjer av:

[Set inn lovleg heimel]

2. **Kategoriar av personopplysningar**

Vi behandlar følgjande kategoriar personopplysningar om deg:

[Spesifiser alle involverte personopplysningar]

3. **Mottakarar eller kategoriar av mottakarar**

Vi vidaresender og gjev dine personopplysningar til desse mottakarane:

[Spesifiser alle mottakarar av opplysningane]

4. **Mottakarar i tredjeland, derunder internasjonale organisasjonar**

Andre land og organisasjonar som vil vere mottakarar av dine personopplysningar:

[Spesifiser om dette er aktuelt. Om dette ikkje er aktuelt opplyser du også om dette]

5. Korleis vi oppbevarer personopplysningane

Vi oppbevarer dine personopplysningar i følgande tidsrom:

[Skildre kor lenge dei blir lagra]

[Om det ikkje er mogleg å angi dette, bruk følgjande tekst:]
Vi kan på noverande tidspunkt ikkje seie kor lenge vi kjem til å oppbevare dine personopplysningar. Dette vil vere i medhald av krava i *[Set inn Lovheimel]*

6. Kvar kjem personopplysningane frå

Dine personopplysningar er innhenta frå:

[Skildre kva kjelder opplysningane er henta frå]

7. Automatiske avgjerder, derunder profilering

[Berre dersom det er aktuelt]

Vi nyttar automatiske vedtak/ avgjersler, derunder profilering, til bruk for:

[Skildre logikken i dei automatiske avgjerdene/vedtaka og forventa konsekvensar av slik behandling]

8. Retten til å trekkje eit samtykke attende

Du har til ei kvar tid rett til å trekkje eit samtykke tilbake.
Dette kan du gjere ved å kontakte dei ovannemnde kontaktpersonane.

Dersom du vel å trekkje tilbake ditt samtykke, påverkar ikkje dette lovlegheita av vår behandling av dine personopplysningar på grunnlag av eit tidlegare underretta samtykke, og fram til tidspunktet for tilbaketrekkinga. Dersom du trekkjer attende ditt samtykke, har det først verknad frå tidspunktet du opplyste oss om at du trakk det attende.

9. Dine rettar

a. Innsynsrett

Du har rett til å få innsyn i dei personopplysningar vi behandlar om deg, samt ei rekkje andre opplysningar.

b. Korrigering

Dersom du ser at nokon av opplysingane ikkje er korrekte, eller du meiner dei treng å supplerast kan du krevje at kommunen rettar opplysingane. Du fyl då ut skjemaet «retting av personopplysning» som ligg på *[Set inn lenkje til skjema]*, eller tek kontakt med kommunen på *[Set inn lenkje til eDialog]*

c. Sletting

Du skal ha rett til å få sletta opplysingar som deg sjølv utan ugrunna opphald dersom:

- Formålet med personopplysingane er innfridd
- Du trekk tilbake samtykket som du har gitt for behandling av personopplysingar, og det ikkje ligg føre noko anna behandlingsgrunnlag
- Du har protestert mot behandlinga/kome med innseiing, og det ikkje fins meir tungtvegande berettiga grunnar til fortsatt behandling, eller opplysingane vert brukt i marknadsføring
- Personopplysingane vert behandla ulovleg
- Personopplysingane må slettast for å oppfylle ei rettsleg forplikting etter EU-retten eller norsk rett som kommunen er underlagt
- Opplysningane er samla inn i samband med informasjonstenester basert på samtykke frå born. (frå 13 år)

Du fyl då ut skjemaet «Sletting av personopplysning» som ligg på *[Set inn lenkje til skjema]* eller du kan ta kontakt med kommunen *[Set inn e-post]* for å få tilsendt skjema.

Ein gjer her merksam på at kommunen som forvaltningsorgan har plikt til å ha arkiv. Det kan difor vere at ein er plikta til å arkivere dine personopplysingar. Dette er eit anna formål enn opplysingane er samla inn for, men vil etter forordninga om personvern ikkje vere i strid med opphaveleg formål, og difor vere lovleg. Kommunen har også plikt etter rekneskapslova å oppbevare nokre opplysingar. Desse kan difor ikkje slettast.

d. Avgrensa behandling

Avgrensa behandling vil seie at du under gitte vilkår kan krevje at kommunen merkar dei opplysingane dei har om deg, slik at desse ikkje vert behandla, altså brukt i t.d. saksbehandling osv.

Du kan krevje avgrensing behandling av personopplysingar dersom:

- du meiner at opplysningane er feil
- du meiner at behandlinga er ulovleg og du ikkje ønskjer sletting
- du meiner at kommunen ikkje lenger treng opplysningane fordi formålet med behandlinga er oppfylt, men du har behov for dei for å fastsette eller gjere gjeldande eller forsvare eit rettskrav
- du har kome med innseiingar mot behandlinga og ein ventar på kontroll av kor vidt kommunen kan behandle opplysingane.

Dersom du ønskjer å krevje avgrensa behandling, fyl du ut skjemaet «avgrensa behandling» som ligg på *[Set inn lenkje til skjema]* eller du kan ta kontakt med kommunen *[Set inn e-post]* for å få tilsendt skjema.

e. Motføresegner mot behandling

Du har til ei kvar tid rett til å protestere mot behandling av personopplysingar om deg som har blir gjort på grunnlag av ei interesseavveging mellom kommunen si interesse og din rett til personvern. Vidare har du rett til å protestere mot behandling av personopplysingar som blir gjort på grunnlag av at det er naudsynt for å utføre ei oppgåve i ålmenta si interesse eller utøve offentleg mynde som kommunen er pålagt.

Dersom du ønskjer informasjon om dine personopplysingar behandla på grunnlag av ei interesseavveging, ta kontakt med kommunen sitt personvernombod *[Set inn kontaktinformasjon]*

Dersom du ønskjer å protestere mot behandling fyl du ut skjemaet «protestere mot behandling» som ligg på *[Set inn lenkje til skjema]* Du kan også ta kontakt med kommunen på: *[Set inn e-post]* for å få tilsendt skjema.

10. Klage til Datatilsynet

Du har rett til å klage til Datatilsynet om du ikkje er nøgd med den måten vi behandlar dine personopplysningar på. Du finn Datatilsynet sine kontaktopplysningar på: www.datatilsynet.no

Har du spørsmål kan du kontakte: *[Set inn kontaktdetaljar]*

Med venleg helsing

[Set inn namn på den behandlingsansvarlege]

15.1.3 Mal –Samtykkeskjema - samtykke som rettsleg grunnlag for behandling av personopplysningar

Samtykkeskjema etter LOV-2018-06-15-38 Lov om behandling av personopplysningar og forordning (EU) 2016/679 om personvern

[Dette er ein mal som kan nyttast til å hente inn samtykke i di verksemd. Denne malen kan redigerast til dykkar unike bruk. Meiningsberande innhald i denne malen skal ikkje endrast.

Samtykkeskjema må lagrast på ein egna stad så lenge samtykket eksisterer.
For meir informasjon sjå eigen rettleiar om samtykke.
All hjelpetekst er i dette formatet, og skal fjernast før bruk.]

NAMN:

FØDSELSDATO:

samtykker med dette i at *[Set inn namn]*kommune kan innhente og behandle personopplysningane mine i samband med: *[skildre kva formålet med behandlinga er, for eksempel behandling av krav, etc.]*

1.
2.
3. etc.

☐ Eg samtykker i at *[Set inn namn]* kommune kan innhente opplysningar frå desse einingane/institusjonane *[Vi må informere om kva einingar/ institusjonar dette er]*

1.

2.

3.

Etc.

☐ Eg samtykker i at følgande opplysningar kan innhentast:
[Namn, personnummer, helseopplysningar, opplysningar frå skule, PPT, barnehage, barnevern, NAV, arbeidsgjevar, etc.]

[Berre dersom det er aktuelt og opplysningar blir utlevert:]

☐ Eg samtykker i at mine personopplysningar kan utleveras til:
[Skildre kva for einingar, private og offentlege, som kan få dine opplysningar]

☐ Eg er kjend med at det er frivillig å gje samtykke og at eg når som helst kan trekke mitt samtykke attende. *[Merk! Dersom vi ønsker å ta bilete eller lage ein opplæringsvideo der fleire personar opptrer, kan det vere umogeleg å få sletta vedkomande i ettertid.*
Det må informerast spesifikt om dette i slike tilfelle]

Eg er vidare kjend med at kommunen berre behandlar og oppbevarer mine personopplysningar så lenge det er naudsynt.

☐ Tidsavgrensa samtykke. Eg samtykker i at mine opplysningar kan behandlast til *[dato]*

Dato/sted:

Signatur:

Sjå vår nettside [Set inn lenkje] for meir informasjon om din rett til mellom anna innsyn, sletting og korrigering.

Personvernombod i kommunen er: [Set inn namn og kontaktdetaljar]

Tilbakekall av samtykke

☐ Eg trekk attende mitt samtykke til

Dato/stad:

Signatur:

15.2 Malar - Rutine for Innsyn etter personvernlova

15.2.1 Mal - Svar i høve krav om innsyn

[MAL – HUGS Å FJERNE ALL HJELPETEKST SOM ER I DETTE FORMATET!]

[Språket i brevet må tilpassast mottakar (døme born, personar med særskilde utfordringar)]

Vi viser til krav datert *[Set inn dato]* om innsyn i dei opplysningar som vert behandla hjå *[Set inn namn på behandlingsansvarleg]*

Vi forstår ditt krav som eit krav om innsyn etter lov om personopplysningar jf. personvernforordninga artikkel 15.

Vi kan opplyse om at vi behandlar personopplysningar om deg. Ein kopi av personopplysningane følgjer vedlagt i bilag 2.

Vidare skal vi i høve ditt krav opplyse om vår behandling av dine personopplysningar.
Dei opplysningar vi pliktar å gje er mellom anna:

1. Formålet med, og det rettslege grunnlaget for behandlinga av dine personopplysningar
2. Kategoriar av personopplysningar
3. Mottakarar eller kategoriar av mottakarar
4. Mottakarar i tredjeland, derunder internasjonale organisasjonar
5. Korleis vi oppbevarer personopplysningane (derunder tidsrom)
6. Kvar personopplysningane kjem i frå
7. Automatiske avgjerder, derunder profilering
8. Rett til korrigering, sletting, avgrensa behandling og innvendingar
9. Klage til Datatilsynet

Dine rettar:

Vi gjer her merksam på at vi som kommune har plikt til å ha arkiv. Det kan difor vere at vi må arkivere (oppbevare) dine personopplysingar. Dette er eit anna formål enn opplysingane er samla inn for, men vil etter forordninga om personvern ikkje vere i strid med opphaveleg formål, og difor vere lovleg. Kommunen har også plikt etter rekneskapslova å oppbevare nokre opplysingar. Desse kan difor ikkje slettast.

Retten til å trekkje eit samtykke attende

Du har til ei kvar tid rett til å trekkje eit samtykke tilbake. Dette kan du gjere ved å kontakte kommunen.

Dersom du er i tvil om kommunen behandlar dine opplysningar på bakgrunn av samtykke, sjå punkt 1 i dette brevet. Her går det fram på kva grunnlag vi behandlar dine personopplysningar.

Dersom du vel å trekkje tilbake ditt samtykke, påverker ikkje det lovlegheita av vår behandling av dine personopplysningar på grunnlag av eit tidlegare underretta samtykke, og fram til tidspunktet for

tilbaketrekkinga. Dersom du trekkjer attende ditt samtykke, har det først verknad frå tidspunktet du underretta at du trakk det attende.

Innsynsrett

Du har rett til å få innsyn i dei personopplysningar vi behandlar om deg, samt ei rekkje andre opplysningar.

Korrigering

Dersom du ser at nokon av opplysingane ikkje er korrekte, eller du meiner dei treng å supplerast, kan du krevje at kommunen rettar opplysingane. Dette gjer du med eDialog *[Set inn lenkje til eDialog]*, eller ved å ta direkte kontakt med kommunen.

Sletting

Du som den registrerte, skal ha rett til å få sletta opplysingar om deg sjølv, utan ugrunna opphald dersom:

- formålet med personopplysingane er innfridd
- Du trekk tilbake samtykket som du har gitt for behandling av personopplysing, og det ikkje ligg føre noko anna behandlingsgrunnlag
- Du har protestert mot behandlinga/kome med innvendingar, og det ikkje fins meir tungtvegande berettiga grunnar til fortsatt behandling eller opplysingane vert brukt i marknadsføring
- Personopplysingane vert behandla ulovleg
- Personopplysingane må slettast for å oppfylle ein rettsleg forplikting etter EU-retten eller norsk rett, som kommunen er underlagt
- Opplysingane er samla inn i samband med informasjonstenester basert på samtykke frå born. (frå 13 år)

Dette gjer du med eDialog *[Set inn lenkje til eDialog]*, eller ved å ta direkte kontakt med kommunen.

Avgrensa behandling

Avgrensa behandling vil seie at du under gitte vilkår kan krevje at kommunen merkar dei opplysingane dei har om deg, slik at desse ikkje vert behandla, altså brukt i t.d. saksbehandling osv.

Du kan krevje avgrensing av behandling av personopplysingar dersom:

- Du meiner at opplysingane er feil
- Du meiner at behandlinga er ulovleg og du ikkje ønskjer sletting
- Du meiner at kommunen ikkje lenger treng opplysingane, fordi formålet med behandlinga er oppfylt, men du som registrert har behov for dei for å fastsette eller gjere gjeldande eller forsvare eit rettskrav
- Du har kome med innvendingar mot behandlinga og ein ventar på kontroll av kor vidt kommunen kan behandle opplysingane.

Dersom du ønskjer å krevje avgrensa behandling, nyttar du eDialog *[Set inn lenkje til eDialog]*, eller ved å ta direkte kontakt med kommunen.

Innvending mot behandling

Du har til ei kvar tid rett til å protestere mot behandling av personopplysingar om deg, som har blitt gjort på grunnlag av ei interesseavveging mellom kommunen si interesse og din rett til personvern. Vidare har du rett til å protestere mot behandling av personopplysingar som blir gjort, på grunnlag av at det er naudsynt for å utføre ei oppgåve i ålmenta si interesse, eller utøve offentleg mynde som kommunen er pålagt.

Dersom du ønsker informasjon om dine personopplysingar behandla på grunnlag av ei interesseavveging, ta kontakt med kommunen sitt personvernombod:

[Set inn kontaktinformasjon]

Dersom du ønskjer å protestere mot behandling, kan du nytte edialog *[Set inn lenkje til eDialog]*, eller ved å ta direkte kontakt med kommunen.

Klage til Datatilsynet

Du har rett til å klage til Datatilsynet om du ikkje er nøgd med den måten vi behandlar dine personopplysningar på. Du finn Datatilsynet sine kontaktopplysningar på: www.datatilsynet.no.

Har du spørsmål, kan du kontakte *[Set inn kontaktdetaljar til behandlingsansvarleg]*

Med venleg helsing

[Set inn namn på behandlingsansvarleg]

Bilag 1 Opplysningar om kommunen si behandling av dine personopplysningar

Bilag 2 Kopi av personopplysningar som er behandla i kommunen

15.3 Malar – Rutine for sletting, korrigering eller avgrensa handsaming av personopplysningar

15.3.1 Mal - Svarbrev – sletting

Mal - svar i høve krav om sletting

[MAL – HUGS Å FJERNE ALL HJELPETEKST SOM ER I DETTE FORMATET!]

[Språket i brevet må tilpassast mottakar
(døme born, personar med særskilde utfordringar)]

Vi viser til krav om sletting datert *[Set inn dato]* av opplysingar som vert behandla hjå *[Set inn namn på behandlingsansvarleg]*

Vi forstår ditt krav som eit krav om sletting etter LOV-2018-06-15-38 Lov om behandling av personopplysninger § 1 jf. personvernsforordninga sin artikkel 17.

[vel alternativ A eller B]

A) Ved semje om at opplysingane skal slettast

Vi har no sletta følgjande personopplysingar om deg:

[Fyll inn relevant informasjon]

B) Ved usemje om at opplysingane skal slettast:

Etter arkivlova kan ikkje kommunen slette opplysingane.
Vi vil tilføye dine synspunkt i saka slik at det kjem fram at du har kravd opplysingane korrigert / komplementert og kva du har kravd korrigert/komplementert.

Vi gjer merksam på at dersom kommunen har vidareformidla ukorrekte opplysingar om deg til ein tredjepart skal kommunen på eige initiativ underrette ev. tredjepart om at opplysingane har vorte korrigert / komplementert og kva som ligg i dette.

Med venleg helsing

[Set inn namn] kommune

15.3.2 Mal - svarbrev i høve krav om korrigering

[MAL – HUGS Å FJERNE ALL HJELPETEKST SOM ER I DETTE FORMATET!]

[Språket i brevet må tilpassast mottakar
(døme born, personar med særskilde utfordringar)]

Vi viser til krav datert *[Set inn dato]* om korrigering av opplysingar som vert behandla hjå *[Set inn namn på behandlingsansvarleg]*

Vi forstår ditt krav som eit krav om korrigering etter LOV-2018-06-15-38 Lov om behandling av personopplysninger § 1 jf. personvernsforordninga sin artikkel 16

[vel alternativ A eller B]

A) Ved semje om at opplysingane skal korrigerast

Vi har no korrigert følgjande personopplysingar om deg:

[Fyll inn relevant informasjon]

B) Ved usemje om at opplysingane skal korrigerast eller ved usemje om opplysingar i faglege / skjønnsmessige vurderingar:

Kommunen sin saksbehandlar er av den faglege oppfatning at opplysingane kommunen behandlar om deg er korrekte og fullstendige. Opplysingane vil difor ikkje verte korrigert. Vi vil tilføye dine synspunkt i saka slik at det kjem fram at du har kravd opplysingane korrigert / komplementert og kva du har kravd korrigert / komplementert.

Vi gjer merksam på at dersom kommunen har vidareformidla ukorrekte opplysingar om deg til ev. mottakarar, skal kommunen på eige initiativ underrette ev. mottakarar om at opplysingane har vorte korrigert / komplementert og kva som ligg i dette.

Ta kontakt med kommunen om du ynskjer informasjon om kommunen har vidareformidla opplysingar til ein tredjepart.

Med venleg helsing

[Set inn namn] kommune

15.3.3 Mal - svarbrev i høve krav om avgrensa behandling av dine personopplysningar

[MAL – HUGS Å FJERNE ALL HJELPETEKST SOM ER I DETTE FORMATET!]

[Språket i brevet må tilpassast mottakar
(døme born, personar med særskilde utfordringar)]

Vi viser til krav datert *[Set inn dato]* om avgrensa behandling av dine personopplysningar hjå *[Set inn namn på behandlingsansvarleg]*

Vi forstår ditt krav som eit krav om avgrensa behandling etter LOV-2018-06-15-38 Lov om behandling av personopplysninger § 1 jf. personvernsforordninga sin artikkel 18.

[vel alternativ A eller B]

A) Ved semje om avgrensa behandling

Vi er einige i at du har rett til avgrensa behandling. Vi legg til grunn at:

A) Du har kravd korrigering / sletting av opplysningar om deg og medan det kravet blir behandla vil vi sjå bort frå dei aktuelle opplysningane
B) Du har motsett deg sletting av personopplysningar til trass for at tidlegare behandling ikkje var lovleg. Vi vil behandle desse opplysningane avgrensa.
C) Du har behov for opplysningane for å fastsetja, gjere gjeldande eller forsvare eit rettskrav, men kommunen har ikkje lenger behov for opplysningane.
D) Du har protestert mot behandling av dine personopplysningar, og medan protesten vert behandla vil vi sjå bort frå desse opplysningane.

Opplysningane dette gjeld er:

[Fyll inn relevant informasjon]

B) Ved usemje om at opplysingane skal behandlast avgrensa:

Dei særskilde vilkåra som må vere oppfylt for at du skal ha rett til avgrensa behandling er:

A) Du har kravd korrigering / sletting av opplysningar om deg, og medan det kravet blir behandla krev du avgrensa behandling av dine personopplysningar.
B) Du har motsett deg sletting av personopplysningar til trass for at tidlegare behandling ikkje var lovleg.
C) Du har behov for opplysningane for å fastsetja, gjere gjeldande eller forsvare eit rettskrav, men kommunen har ikkje lenger behov for opplysningane.
D) Du har protestert mot behandling av dine personopplysningar, og medan protesten vert behandla krev du avgrensa behandling.

Kommunen finn ikkje at nokon av disse vilkåra er oppfylt.

[ELLER]

Kommunen finn at du fyller vilkåra, men det er naudsynt for kommunen å behandle desse opplysningane for å

- fastsetje, gjere gjeldande eller forsvare eit rettskrav
- verne ein annan fysisk eller juridisk person sine rettar
- verne viktige ålmente interesser

Vi gjer merksam på at dersom kommunen har vidareformidla ukorrekte opplysingar om deg til ev. mottakarar skal kommunen på eige initiativ underrette ev. mottakarar om at opplysingane har vorte korrigert / komplementert og kva som ligg i dette.

Ta kontakt med kommunen om du ynskjer informasjon om kommunen har vidareformidla opplysingar til ein tredjepart.

Med vennleg helsing

[Set inn namn] kommune

15.4 Malar - Rutine når den registrerte protesterer mot behandling av personopplysningar i kommunen

15.4.1 Mal - svar i høve protest mot behandling av personopplysningar

[MAL – HUGS Å FJERNE ALL HJELPETEKST SOM ER I DETTE FORMATET!]

Vi viser til e-post / brev av *[Set inn dato]* med protest mot behandling av personopplysningar som vert behandla hjå *[Set inn namn på behandlingsansvarleg]*

Vi forstår din/ditt e-post/brev slik at du protesterer mot at kommunen skal behandle dine personopplysningar etter LOV-2018-06-15-38 Lov om behandling av personopplysningar § xx jf. personvernforordninga sin artikkel 16.

[fyll inn det som passar, alternativ A eller B]

C) Ved semje om at kommunen ikkje skal behandla opplysingane om den registrerte

Kommunen har vurdert dine rettar etter personvernreglane. Kommunen har etter ei totalvurdering kome til at dine rettar veg tyngre enn kommunen si plikt i denne saka.
Vi har då særleg lagt vekt på *[Forklar kort kva kommunen har lagt vekt på]*

Kommunen stansar behandlinga av dine personopplysningar i denne saka.

D) Ved usemje i at kommunen ikkje har tilstrekkeleg grunnlag for å behandle personopplysningane:

Kommunen sin saksbehandlar er av den faglege oppfatning at:

[Vel det som er aktuelt under]

- Kommunen har ei legitim plikt til å behandle personopplysningar om deg angi kva for lovgrunnlag som gjeld
- Behandling av dine personopplysningar er naudsynt for å fastsette, gjere gjeldande eller forsvare eit rettskrav
- Det er i ålmenta si interesse å behandle dine personopplysningar for vitskapelege eller statistiske føremål.

Med vennleg helsing

[Set inn namn] kommune