VINDAFJORD KOMMUNE

VITAL & SENTRAL

INTERNKONTROLL

Personopplysningar og datatryggleik

Foreløpig versjon 1-2019

Innhald

Innleiing frå rådmannen

Ny personopplysningslov blei vedtatt i 2018. Lova består av nasjonale reglar og EUs personvernforordning (GDPR - General Data Protection Regulation). Forordninga er eit sett reglar som gjeld for alle EU/EØS-land.

Personopplysningslova handlar om behandling – altså innsamling og bruk – av personopplysningar. Reglane gir verksemdene ei rekkje plikter samtidig som den gir enkeltpersonar, ofte kalla registrerte, ei rekkje rettar.

Personopplysningslova kan skisserast på følgjande måte:

1. Nasjonale reglar med norske tilpassingar (kapittel 1-9)

2. EUs personvernforordning, som består av to delar:

Fortale. Dette er ei tolkingshjelp som kan utfylla eller forklara artiklane.
Artiklar (Kapittel I-XI). Her finnes dei fleste personvernreglane i personopplysningslova. Det er berre artiklane som er juridisk bindande.

Det følgjer av både personopplysningslova og EØS-lova at personvernforordninga skal gå framfor norsk lov ved konflikt. Det betyr at alle norske reglar om behandling av personopplysningar må passa inn i personvernforordninga sitt system for å vera gyldige.

Personvernforordninga er lik for alle EU/EØS-land. Verksemder, etablert i andre EU/EØS-land, må derfor stort sett følgja dei same personvernreglane som norske verksemder.

I ein periode framover vil det gjelda overgangsreglar, jf. forskrift *FOR-2018-06-15-877*

Elles tryggjar også andre lovar personvernet. Dette er særlovgiving som inneheld nasjonale tilpassingar innan ulike sektorar, slik som pasientjournallova, politiregisterlova og liknande.

Vindafjord kommune er avhengig av å behandla personopplysningar for å administrera og forvalte forholdet til våre tilsette, og forholdet til våre brukarar. Rådmannen er behandlingsansvarleg, og ansvarleg for at behandlinga av personopplysningar og informasjon skjer etter personopplysningslova sine krav.

Den *behandlingsansvarlege* bestemmer formålet med behandlinga av personopplysningar og kva hjelpemiddel som skal brukast. Dette er vanlegvis ei verksemd (Personvern-forordninga artikkel 4, nr 7). Det er den behandlingsansvarlege som har ansvaret for at personvernlovgivinga vert følgd.

Alle offentlege verksemder skal ha eit *personvernombod*. Personvernombodet si hovudoppgåve er å informera og gi råd om dei pliktene kommunen har etter personvernlovgivinga til den behandlingsansvarlege eller databehandlaren, samt til dei tilsette som utfører behandlinga av personopplysningar.

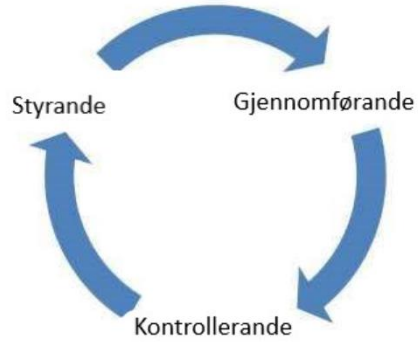
I personvernforordninga sin artikkel 39 gis det dessutan ei oversikt over ei rekkje andre oppgåver eit personvernombod har.

Artikkel 30 gir pålegg om at den behandlingsansvarlege skal føre skriftleg og elektronisk protokoll over behandlingsaktivitetar som blir utført under deira ansvar. Vindafjord kommune sin protokoll blir for tida ført i det elektroniske systemet Draftit.

Vindafjord kommune sitt system for å ivareta vårt ansvar etter personopplysningsloven, blir presentert i dette dokumentet. Arbeidet er også gjennomført for å svare opp på forvaltningsrevisjon om IKT og informasjonstryggleik av august 2018.

Kommunen må sikra ein forsvarleg behandling av personopplysningar ved at me tar vare på den registrerte sin rettar og fridomar, samtidig som me tar vare på kommunen sine mål ved behandlinga. Etter personvernforordninga (artikkel 24) inneber det at me rett avpassar og ser på art, omfang, formål og samanheng, samt risikoane for fysiske personar sine rettar og fridomar ved behandlinga, og ut frå det gjennomfører eigna tekniske og organisatoriske tiltak. Internkontroll skal vera leiinga sitt verktøy for å ivareta sitt ansvar og demonstrera etterleving av personvernregelverket, og dei tilsette sitt verktøy for å utføra oppgåver på ein forsvarleg og sikker måte. Tiltaka skal dokumenterast og oppdaterast etter behov.

Systemet er i hovudsak bygd opp etter Datatilsynet sin rettleiar om Internkontroll og informasjonstryggleik, så langt den passar med vår verksemd. Systemet er samansett av tre delar:



Styrande element, som i hovudsak rettar seg mot leiinga, og kva avgjersler og føringar dei legg for internkontroll.
Gjennomførande element, som i hovudsak rettar seg mot tilsette. Her finn ein framstilling av rutinar som er tilpassa den enkelte sin arbeidssituasjon.
Kontrollerande element, som bidrar til å fanga opp avvik frå systemet og til at det vert gjennomført periodiske gjennomgangar.

Behandling av eventuelle avvik vil kunne medføra justeringar i både *styrande* og *gjennomførande* element. På denne måten får kommunen eit rullerande system, som forsøkt vist i figuren over.

Me behandlar sensitive opplysningar som treng høg grad av vern. Det ligg i vår oppgåve som tenesteleverandør av viktige tenester for alle livets fasar. Sjølv om Vindafjord kommune er underlagt offentleglova, må det visast utstrekt grad av varsemd i praktiseringa for å sikre at fortruleg informasjon ikkje kjem ut.

Beskrivingane gjeld krav og plikter som kommunen er underlagt på grunn av personopplysningar, og eventuelle krav og plikter gjennom andre lover og forskrift er.

Styringsdokument og underliggande dokumenter er godkjent av rådmannen ……, og blir forutsett følgd opp av alle som behandlar fortruleg informasjon.

Ølen, den

Rådmann

Generelt om behandling av personopplysningar

All *behandling av personopplysningar* må ha eit rettsleg grunnlag for å vera lov (jf. personvernforordninga artikkel 6). Det betyr at me på forhånd må ha identifisert om det finnes eit *behandlingsgrunnlag*. Viss ikkje det finnes, er behandlinga ulovleg.

I utgangspunktet er det forbode å behandla visse kategoriar av personopplysningar. Mange omtalar desse opplysningstypane som *sensitive personopplysningar*.

Opplysningskategoriane dette gjeld er:

1. opplysningar om rase eller etnisk bakgrunn
2. opplysningar om politisk oppfatning
3. opplysningar om religion
4. opplysningar om filosofisk overtyding
5. opplysningar om fagforeiningsmedlemskap
6. genetiske opplysningar
7. biometriske opplysningar med det formål å eintydig identifisera nokon
8. helseopplysningar
9. opplysningar om seksuelle forhold
10. opplysningar om seksuell legning
11. opplysningar om straffedommar
12. opplysningar om lovbrot

Det finnes mange unntak frå forbodet. Etter lova må det føreliggja eit særskilt grunnlag i tillegg til behandlingsgrunnlag for å behandla denne typen opplysningar.
I forordninga (artikkel 9 nr. 2 og 3) er det ei oversikt over når opplysningane i punkt 1 til 10 likevel kan behandlast. Nedanfor er det ei forenkla oppsummering av denne oversikta. Det er viktig å understreka at det er mange atterhald, så ein må uansett setja seg inn i forordningsteksten før ein eventuelt set i gang behandlinga av personopplysningar:

- Den registrerte har gitt uttrykkeleg samtykke.
- Behandlinga er nødvendig for at den behandlingsansvarlege eller den registrerte skal kunna oppfylla og utøva sine arbeidsrettslege, trygderettslege og sosialrettslege plikter og rettar i den grad behandlinga er tillaten etter lov eller tariffavtale.
- Behandlinga er nødvendig for å verna den registrerte eller ein annan person sine vitale interesser viss den registrerte ikkje er i stand til å gi samtykke.
- Behandlinga blir utført av ei stifting, samanslutning eller ideelt organ som har mål av politisk, religiøs eller fagforeiningsmessig art, så lenge det er snakk om personopplysningar om medlemmer og liknande, og opplysningane ikkje blir utlevert utan samtykke.
- Behandlinga gjeld opplysningar som den registrerte sjølv openbart har offentleggjort.
- Behandlinga er nødvendig i forbindelse med rettskrav eller domstolane handlar innanfor ramma av sin domsmynde.
- Behandlinga er nødvendig av omsyn til viktige allmenne interesser og har heimel i lov.
- Behandlinga er nødvendig i forbindelse med førebyggjande medisin, medisin i arbeidslivet, vurdering av ein arbeidstakar sin arbeidskapasitet, medisinsk diagnostikk,

yting av helse- eller sosialtenester, sosialfagleg eller medisinsk behandling eller forvaltning av helse- eller sosialtenester og -system. Dette gjeld likevel berre dersom opplysningane blir behandla av ein fagperson underlagt teieplikt, og behandlinga av personopplysningar må ha heimel i lov eller følgja av avtale med helsepersonell.
- Behandlinga er nødvendig av allmenne folkehelseomsyn.
- Behandlinga er nødvendig for arkivformål i allmenn interesse, for formål knytt til vitskapeleg eller historisk forsking eller for statistiske formål, så lenge det føreligg visse tiltak og behandlinga har heimel i lov.

Der forordninga seier at ei behandling av personopplysningar krev heimel i lov, stiller den også visse krav til lova eller ting lova skal innehalde. Det vil sei at ein kva som helst lovheimel i seg sjølv ikkje nødvendigvis er tilstrekkeleg.
I tillegg seier personopplysningslova §§ 6, 7 og 9 at sensitive personopplysningar kan behandlast:

- når det er nødvendig for å gjennomføra arbeidsrettslege plikter eller rettar
- dersom Datatilsynet har gitt høve til det og har fastsett vilkår for å verne den registrerte sine grunnleggjande rettar og interesser
- dersom behandlinga er nødvendig for arkivformål i allmenn interesse, for formål knytt til vitskapeleg eller historisk forsking eller for statistiske formål. Dette gjeld så lenge samfunnet si interesse i at behandlinga finn stad klart overstig ulempene for den enkelte. Det må også føreliggja visse tiltak og ein må ha rådført seg med personvernombodet.

Opplysningane i punkt 11 og 12 kan berre behandlast:

- under ein offentleg styresmakt sin kontroll. Dersom behandlinga er nødvendig for arkivformål i allmenn interesse, for formål knytt til vitskapeleg eller historisk forsking eller for statistiske formål, må likevel verksemda først rådføra seg med personvernombodet.
- med heimel i personopplysningslova § 11
- med heimel i annan norsk lov så lenge lova inneheld garantiar for den registrerte sine rettar og fridomar.

Omfattande registrer over straffedommar kan uansett berre førast under ein offentleg styresmakt sin kontroll.

Styrande dokumentasjon

Styrande dokumentasjon beskriv systemet og inneheld element som policy og målsetjing, identifiserte krav og plikter, intern organisering, ansvar og mynde. Styrande dokumentasjon er overordna i sin form og er spesielt leiingsorientert.

Sentrale lover og forskrifter

Informasjonstryggleiken i kommunen er regulert av ei rekkje lovar og regler. Dette er nokre av dei mest sentrale:

- Lov om kommunar og fylkeskommunar
- Lov om behandling av personopplysningar (personopplysningslova)
- Lov om behandlingsmåten i forvaltningssaker (forvaltningslova)
- Forskrift om elektronisk kommunikasjon med og i forvaltninga (eForvaltningsforskrifta)

- Lov om rett til innsyn i dokument i offentleg verksemd (offentleglova)
- Lov om nasjonal sikkerhet (sikkerhetsloven), nye forskrifter er under behandling
- Arbeidsmiljølova
- Arkivlova
- Helseregisterlova
- Forskrift om systematisk helse-, miljø- og sikkerheitsarbeid i verksemder (Internkontrollforskrifta)

Tryggleiksmål

Vindafjord kommune si behandling av informasjon skal vera i samsvar med regulatoriske, interne og avtalerettslege krav til informasjonstryggleik. Personopplysningar og annan verneverdig informasjon skal sikrast på ein trygg måte gjennom fysiske, tekniske og organisatoriske tiltak.

Konfidensialitet
Personopplysningar og annan verneverdig informasjon som blir behandla i kommunen skal vera verna mot uautorisert tilgang.
Personopplysningar blir behandla konfidensielt og kan berre delast med andre medarbeidarar i den grad det er tenestlege behov.
Personopplysningar om eigne arbeidstakarar kan berre bli behandla av den som har tenestleg behov.

Integritet
Informasjon som kommunen har ansvaret for blir berre produsert og endra av tilsette, eller av eksterne som har fullmakt til dette. Informasjon skal ikkje endrast utilsikta.

Tilgjengelegheit
Informasjonssystemet er tilgjengeleg for autoriserte brukarar ved behov.

Robustheit
Kommunen og informasjonssystemet er motstandsdyktig og robust.
Når uønskte fysiske eller tekniske hendingar inntreff, bidrar beredskapstiltak til å avgrense skaden og at kommunen raskt kjem tilbake til normal drift. Dette inkluderer igjen å oppretta tilgjenge og tilgang til personopplysningar i rett tid.

Tryggleiksstrategi

Arbeidet med informasjonstryggleik skal:

- vera forankra i linja og utførast systematisk
- gjennomførast for å nå måla for informasjonstryggleik
- vera risikobasert og følgja kjente standardar
- følgje prinsippa for læring og kontinuerleg forbetring

Det inneber at:

- risikovurderingar blir gjennomført systematisk, periodisk og ved vesentlege endringar i oppgåver eller omgivnadar
- tiltak for å redusera risiko er basert på risikovurderingar og leiinga sine føringar for risikohandtering og akseptabel risiko

- hendingar som ut frå risiko kan påverka informasjonstryggleiksmåla negativt, blir melde og følgd opp på ein systematisk måte
- leiinga systematisk styrer og følgjer opp informasjonstryggleiksarbeidet
- leiinga systematisk følgjer opp måloppnåing, etterleving, kompetanse og kultur.

For å lykkast med dette skal alle tilsette:

- ha eit bevisst forhold til kommunen sine tryggleiksmål og kor viktige dei er
- vite kva typar informasjon dei behandlar og kva krav som blir stilt til deira eigen informasjonsbehandling og bruk av IKT
- etterleva krav, retningslinjer, prosedyrar, rutinar osv. som gjeld for dei og det arbeidet dei utfører.

Strategiane skal implementerast gjennom informasjonstryggleiksutvalet (ITU).

Tryggleiksval

Systemteknisk tryggleik – nødvendig tryggleiksnivå

Avhengig av det aktuelle systemet og informasjonen som behandlast, vil dei ulike aspekta ved tryggleik (konfidensialitet, integritet, tilgjengelegheit og robustheit) ha ulik betydning. Følgjande kategorisering blir nytta for vernebehov:

- **Høg** – blir gitt system og informasjon med kritisk vernebehov for kommunen
- **Middels** – blir gitt system og informasjon med vernebehov
- **Låg** (låge krav til tryggleik) – kan gjelde alle system og informasjon med lite eller ingen vernebehov.

Ulike delsystem kan ha ulike vernebehov.

Tekniske tryggleikstiltak

- Tiltak som forhindrar at arbeidstakarar uaktsamt eller med forsett skal kunna skade informasjonssystemet eller informasjon som er lagra her.
- Tiltak som sørger for å gi tilgang til informasjonssystemet for dei brukarane som er autoriserte, og som forhindrar at uvedkommande blir gitt tilgang til informasjon.
- Det er etablert tryggleikslogging for dei systema der det er mogleg, som gjer at tryggleiksbrot på systemnivå kan avdekkast.
- Tiltak som forhindrar at skadeleg programvare kjem inn i kommunen sine informasjonssystem.
- Jamleg tryggleikskopiering av all data som blir lagra på kommunen sine serverar.
- Tapt informasjon skal kunna gjerast tilgjengeleg igjen seinast innan tre arbeidsdagar. I den grad tap av informasjon skyldast brann eller annan alvorleg skade, skal informasjonen kunne gjerast tilgjengeleg seinast innan to veker. For informasjonssystema gjeld det at alvorleg systemfeil (for eksempel svikt i vitale komponentar) ikkje skal føra til driftsstans meir enn 72 timer.
- For telefonsystemet blir det ikkje tillate driftsstans som overstig 24 timar for driftsfeil. Ved alvorlege systemfeil skal feilretting startast utan ugrunna opphald.

Tryggleiksarkitektur

Datatilsynet meiner at tryggleiksarkitektur skal delast inn i åtskilde soner. Ei sone er eit åtskild segment eller del av eit tryggleikssystem med tilhøyrande einingar, som berre kan kommunisera seg imellom. Soner lagast etter at verksemda har kartlagt kva behandlingar verksemda gjer, gjennomført ei risikovurdering av behandlinga, og avklart kva personopplysningar verksemda behandlar:

1. Sikker sone. Sone der sensitive personopplysningar behandlast (ved behov skal det opprettast fleire sikre soner i verksemda). Den enkelte sikre sona skal vera tryggleiksmessig åtskild både frå resten av det interne nettverket og frå eventuelle andre sikra soner. System som ligg i siker sone: Fagsystem for Pleie og omsorg, Lege, Helsestasjon, Flyktning, PPT, Barnevern, NAV Sosial og arkiv for sikker sone.
2. Intern sone. Sone der ikkje-sensitive personopplysingar blir behandla. Denne kan også omfatte andre opplysningar i verksemda som ikkje skal eksponerast eksternt (ved behov skal det opprettast fleire interne soner i verksemda). System som ligg i intern sone: Økonomi, HRM, Kart og kommunal tekniske system, Arkiv mm. Desse systema er verna med streng tilgangsstyring.

Organisatoriske tiltak

- Rutinar for handtering av tilgang til kommunen sine informasjonssystem. I dette ligg kontroll av passord, rettar, applikasjonar osv. Kor vanskelege passorda skal vera blir handtert av systemet og ligg på eit høgt nivå. <*Passordråd finnest her: https://nettvett.no/passord/* >
- Rutinar for tilsette si handtering av transportable lagringsmedium, slik som berbare datamaskinar, for å unngå at informasjon hamnar på avvegar.
- Rutinar for låsing av lokala, handtering av gjester og bruk av alarm utanom arbeidstid.
- Prosedyrar for plassering og sikring av komponentar, lagringsmedium, dokumenter eller andre bestanddelar som er vitale for drifta av kommunen.

Fysiske tiltak

- Kommunen sine lokale blir sikra mot blant anna innbrot, brann, vasskade osv.
- Forhindra at uvedkommande blir gitt tilgang til lokale kor verneverdig informasjon blir oppbevart.
- Maskinpark, lagringsmedium og sentrale nettverkskomponentar er fysisk sikra, slik at uvedkommande ikkje kan bringa dette med seg ut av etaten sine lokale.
- Berbare einingar, som er meint å tas med utanfor kommunen sine lokale, skal sikrast med kryptering.
- System for destruksjon av sensitive opplysningar. Det finnest eigen deponeringskasse som er tilstrekkeleg verna slik at ikkje dokument kan fjernast etter deponering. Like eins finnes det et tilfredsstillande system for handtering av elektroniske lagringsmedium.

Kommunen er ikkje oppe på nivået som er beskrive ovanfor overalt, men vil vurdere tiltak på desse områda etter forslag frå Informasjonstryggleiksutvalet (ITU) i framtidige budsjett.

Bruk av databehandlarar og underleverandørar

Kommunen sin bruk av databehandlarar og leverandørar skal regulerast i kontraktar, kor også

bestemmingar om informasjonstryggleik inngår. Alle avtalar kor ei ekstern verksemd tar på seg oppdrag for kommunen, som også omfattar informasjonstryggleik, skal baserast på avtalar som minst samsvarer med krava som er gitt i personvernforordninga artikkel 28 og 29. Systemeigar/Einingsleiar kan ikkje engasjera nye leverandørar utan at dette blir avklart med arkivleiar og IT-sjef. Eksterne verksemder eller personar kan ikkje bli gitt tilgang til kommunen sine informasjonssystem med mindre dette skjer som ledd i ein godkjent avtale. ITU har ansvar for å leggja fram problemstillingar knytt til databehandlaravtalar for leiinga.

Organisering

Rådmannen har overordna ansvar for kommunen sin informasjonstryggleik. Den formelle ansvarsorganiseringa følgjer tenesteveg frå rådmann til den einskilde tilsette. Ansvarsoppfølging er delegert til kommunalsjefar og leiarar.

Ansvarsfordeling

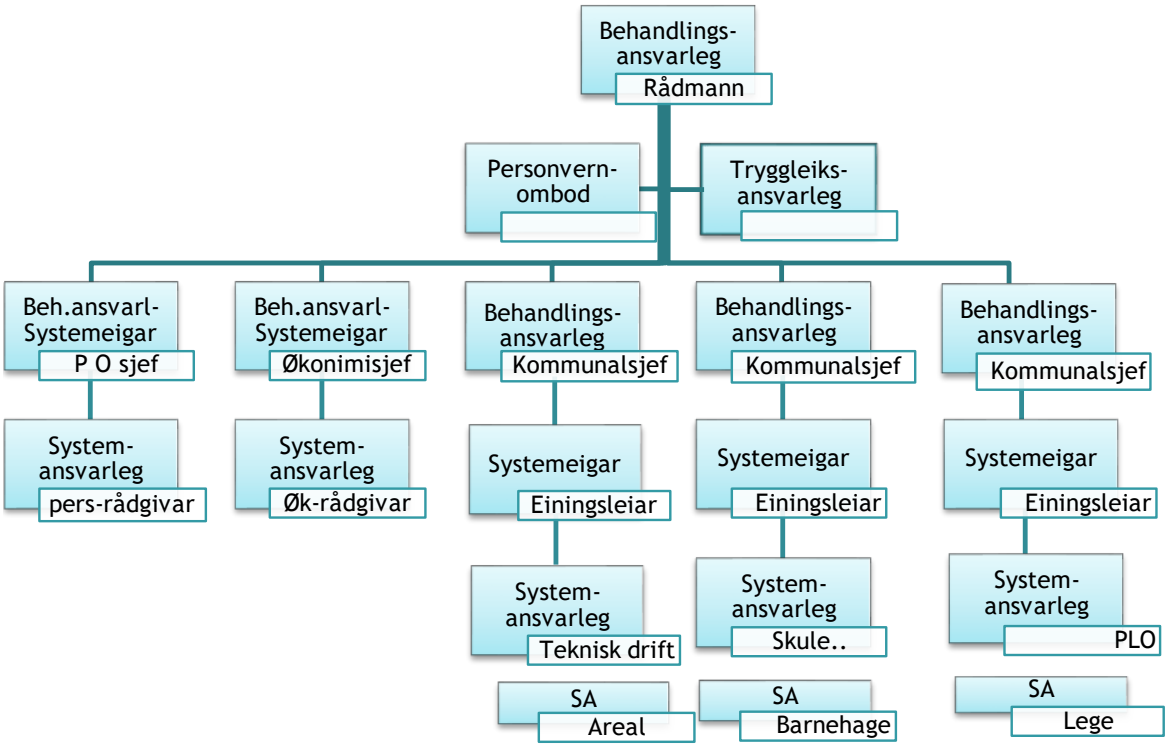
Ansvar er og organisert ut frå funksjonsroller. Alle tilsette har ansvar for at informasjonstryggleiken i kommunen blir varetatt på ein god nok måte.

Viktige føresetnader og prinsipp

- Alle tilsette skal ha kjennskap til kven som er ansvarleg for tryggleiken i det systemet dei nyttar, kva rutinar som er fastsett, og korleis avvik eller forslag til forbetring skal rapporterast.
- Leiarar er ansvarlege for at dei han/ho har personalansvar for har naudsynt kompetanse og rammevilkår for å kunna ivareta informasjonstryggleik i tenesta.
- Leiarar kan delegera mynde til dagleg varetaking av ansvar, men ikkje sjølve ansvaret.
- Leiarar kan delegera til funksjonsnivå, t.d. kan ein leiar som er systemeigar delegere mynde til ein systemadministrator for å sikra at krav i lover og forskrifter blir etterlevd i praksis.

Tryggleiksorganisasjonen

Kartet nedafor viser kommunen sin tryggleiksorganisasjon. Rådmannen er behandlingsansvarleg for kommunen. Ansvaret blir utøvd gjennom kommunalsjefane, økonomisjef og personal- og organisasjonssjef for deira område. Kommunen oppnemner tryggleiksansvarleg, som rapporterer direkte til rådmannen, så snart det let seg gjera. Inntil tryggleiksansvarleg er på plass, er dette ansvaret plassert hos kommunalsjefane, økonomisjef og personal- og organisasjonssjef for deira område. Personvernombod skal løysast i samarbeid med andre kommunar.



Rådmannen sitt formelle ansvar

Rådmannen er behandlingsansvarleg og det primære pliktsubjektet etter forordninga, er overordna ansvarleg for å overhalde personvernprinsippa og regelverket (artikkel 5), og at behandlinga av personopplysningar skjer på ein lovleg, rettferdig og gjennomsiktig måte. Behandlingsansvarleg skal sikre at kommunen sine plikter i forbindelse med personvernregelverket og innsamling av personopplysningar blir varetatt, slik som at:

- det må liggje føre eit eller fleire klart formulerte formål med behandlinga.
- det må finnast eit behandlingsgrunnlag for behandling av kvar enkelt personopplysning til kvar enkelt formål (artikkel 5.1 bokstav a og artiklane 6 og 9)
- det må kommuniserast på ein kortfatta, open, forståeleg og lett tilgjengeleg måte (artikkel 5, 12, 13 og 14)
- det blir lagt til rette for oppfylla brukaren sine rettar til innsyn og tilgang til eigne personopplysningar (artiklane 12-21)
- brukaren sin rett og kommunen si plikt til retting og sletting blir følgd opp (artiklane 16 og 17)
- det blir oppnemnd eit personvernombod (§§ 8 – 11 i personopplysningslova, artiklane 37-39)
- det blir vurdert personvernkonsekvensar og forhandsdrøfting dersom behandlinga sannsynlegvis vil medføra ein høg risiko for rettane og fridomane til fysiske personar (artikkel 35)
- det tas omsyn til personvern i alle utviklingsfasar av eit system eller ei løysing - innebygd personvern (artikkel 25)
- det gjennom å ha god internkontroll og god informasjonstryggleik sikrar og dokumenterer

at kommunen behandlar personopplysningar lovleg, sikkert og forsvarleg (artikkel 24)
- personopplysningar skal vernast tilfredsstillande mot grunnlaust innsyn og grunnlause endringar, samtidig skal opplysningane vera tilgjengelege for dei som treng opplysningane, når dei har behov for dei
- det blir ført protokoll over behandlingsaktivitetar, som er elektronisk tilgjengeleg (artikkel 30)
- det blir inngått databehandlaravtalar med underleverandørar (artiklane 28 og 29)
- kommunen har klare reglar/rutinar for avvikshandtering og at det blir rapport inn avvik til Datatilsynet så snart som mogleg etter at avviket er oppdaga, og seinast innan 72 timar (artiklane 33 og 34)
- personvernregelverket blir følgd ved overføring av opplysningar til utlandet (artiklane 44-49)

Personvernombod

Personvernombodet si hovudoppgåve er å informera og gi råd om dei pliktene kommunen har etter personvernlovgivinga til den behandlingsansvarlege eller databehandlaren, samt til dei tilsette som utfører behandlinga av personopplysningar.

Kontrollera at personvernregelverket blir følgd

Ombodet skal kontrollera at personvernlovgivinga og andre relevante regelverk innan personvern, samt kommunen sin eigne interne retningslinjer for personvern blir følgd. Som ein del av dette kan ombodet ha følgjande oppgåver:

- samla inn informasjon for å identifisera behandlingsaktivitetar
- analysera og sjekka at behandlingsaktivitetane er i tråd med regelverket
- informera, gi råd og tilrådingar for å sikra at regelverket blir følgd
- foreslå ansvarsfordeling for oppgåver knytt til varetaking av personvernet i kommunen
- gjennomføra haldningsskapande arbeid i kommunen og opplæring av medarbeidarar

Sjølv om personvernombodet har ei rolle i å kontrollera at regelverket blir følgd, er det framleis den behandlingsansvarlege eller databehandlaren som er ansvarleg for at personvernlovgivinga blir følgd.

Gi råd om vurdering av personvernkonsekvensar (DPIA)

Personvernombodet skal på oppmoding gi råd om vurderinga av personvernkonsekvensar (Data Protection Impact Assessment – DPIA) og kontrollera gjennomføringa av konsekvensvurderingane. Det er den behandlingsansvarlege, ikkje personvernombodet, som har ansvar for at slike vurderingar blir gjennomført. Ombodet kan likevel ha ei viktig rolla med å hjelpa den behandlingsansvarlege i desse vurderingane.

Artikkel 35 i forordninga pålegg den behandlingsansvarlege å be om råd frå ombodet når ein konsekvensvurdering skal utførast. Den behandlingsansvarlege kan be om råd om:

- det er behov for å utføra ei vurdering av personvernkonsekvensar
- kva metode som skal nyttast
- konsekvensvurderinga skal gjerast internt eller ved hjelp av eksterne krefter
- kva tryggleikstiltak (tekniske og organisatoriske) som bør tas for å minimere *risiko*
- kor vidt konsekvensvurderingane er blitt gjennomført på rett måte, og om konklusjonane er i tråd med regelverket

Samarbeid med Datatilsynet og funksjon som kontaktpunkt
Personvernombodet skal samarbeida med Datatilsynet og fungera som eit kontaktpunkt for tilsynet ved eventuelle spørsmål. Ved behov skal ombodet også kunne rådføra seg med tilsynet. Ombodet skal legge til rette for at Datatilsynet får den informasjonen det treng for å utføra sine oppgåver og plikter, for eksempel i forbindelse med si kontrollverksemd.
Dei registrerte skal på si side kunna kontakta personvernombodet med alle spørsmål knytt til behandling av deira opplysningar, og om utøving av rettane dei har som følgje av personvernlovgivinga.

Prioritert innsats der personvernrisikoen er høgast
Forordninga forutset at personvernombodet tar omsyn til risikoane behandlingsaktivitetane kan ha, sett i lys av behandlingas art, omfang, formål og samanhengen den blir utført i. Dette betyr at innsatsen frå personvernombodet si side naturleg nok i hovudsak bør rettast mot områder kor risikoen for personvernet blir vurdert å vera høgast.

Hjelpa til med å få oversikt over behandlingane i kommunen
Artikkel 30 i forordninga pålegg den behandlingsansvarlege eller databehandlaren å føra ei oversikt over kva for behandlingar av personopplysningar kommunen har.
Den behandlingsansvarlege kan bestemma å gi ombodet fleire oppgåver, så lenge det ikkje oppstår interessekonflikt. Det å etablere ei slik oversikt er ei oppgåve som ofte vil bli delegert til personvernombodet. Ei slik oversikt er då også eit viktig verktøy for at personvernombodet skal kunne utføra sine oppgåver.

Tryggleiksansvarleg

Tryggleiksansvarleg rapporterer til rådmannen og har ansvar for at fysisk tryggleik, tryggleik rundt arkivering, post og personale. Dette inneber ansvar for:

- tilrettelegging av leiinga si gjennomgang
- oppfølging, korrigering og vedlikehald av regime for Internkontroll/eigenkontroll
- at gjeldande tryggleiksbestemmingar, instruksar og rutinar blir følgt
- at tryggleiksorganisasjonen har klart definerte oppgåver og at det er lagt til rette for at den enkelte kan utøva sine funksjonar, og verkeleg utøver desse
- at administrasjonen utøver sitt ansvar for fysisk tryggleik, personale og tryggleik og dokumenttryggleik
- å utføra inspeksjonar på kontor, møterom og andre lokale, der han/ho finn det nødvendig. Inspeksjonane treng ikkje vera varsla
- å påtala misleghald munnleg eller skriftleg, avhengig av misleghaldets karakter
- å sørga for at alle tilsette har kjennskap til regimet for Internkontroll og tilhøyrande tryggleiksbestemmingar, instruksar og rutinar

Inntil kommunen har oppnemnt tryggleiksansvarleg, ligg ansvaret hos kommunalsjefane, økonomisjef og personal- og organisasjonssjef for deira område.

Kommunalsjefane, økonomisjef og personal- og organisasjonssjef sitt formelle ansvar

Kommunalsjefane, økonomisjef og personal- og organisasjonssjef rapporterer til rådmannen i tryggleikssaker. Dei har delegert behandlingsansvar og er inntil vidare tryggleiksansvarlege for sitt område. Det skal spesielt vektleggast:

- at informasjonstryggleiken vert ivaretatt og at kommunen sin plikter etter personvernforordninga blir følgd opp innan forvaltningsområdet
- at det blir gjennomført risikovurderingar
- at det blir gjennomført vurdering av personvernkonsekvensar (Data Protection Impact Assessment - DPIA)
- at risikoreduserande tiltak blir implementerte
- at dokumentasjon blir oppdatert
- at einingsleiar har rett kompetanse
- å setja i verk kontroll om at tryggleiken vert følgd opp i forvaltningsområdet og gjennomføra prosessar for forbetring
- at ansvarsområda til einingsleiar er beskrive i leiaravtalen

Einingsleiar sitt formelle ansvar

Einingsleiarar rapporterer til kommunalsjef i tryggleikssaker. Einingsleiar er ansvarleg for:

- at informasjonstryggleiken vert ivaretatt og at kommunen sine plikter etter personvernforordninga blir følgd opp i eininga
- At dei tilsette får opplæring om informasjonstryggleik
- at tilsette har rett kompetanse til å utføra sine oppgåver
- at dei tilsette har autorisasjon til å bruka informasjonssystema i samsvar med gjeldande systemrutinar
- å halde seg ajour med endringar i regelverk, utarbeida retningslinjer, etablera og vedlikehalda rutinar, setja i verk eigenkontroll og gjennomføra prosessar for forbetring
- å gjennomføra rutinar for teieplikt (omfang og konsekvens) og arkivera signerte dokument

Einingsleiar skal melda behov for autorisasjonar for nytilsette til systemeigar. Meldingar om autorisasjonar skal arkiverast. Einingsleiar sørger for at tilsette blir fjerna frå systema når dei sluttar.

Den einskilde sitt formelle ansvar

Alle tilsette i Vindafjord kommune har eit sjølvstendig ansvar for å ivareta informasjons-tryggleiken i sitt daglege arbeid. Den einskilde skal;

- følgja gjeldande rutinar for informasjonshandsaming både elektronisk og fysisk (nedlåsing, sikring osv.)
- rapportere eventuelle avvik frå gjeldande rutinar, og/eller foreslå forbetringar
- rapportera til leiar i tryggleikssaker

Ansvar som er knytt til funksjonsroller

«Informasjonstryggleiksutvalet» (ITU)

Det blir oppnemnd eit felles Informasjonstryggleiksutval for Etne og Vindafjord kommunar. Tryggleiksansvarleg(e), IT-sjef er medlemmer i utvalet. I tillegg oppnemner Vindafjord 3 og Etne 2 medlemmer til utvalet. Desse skal dekka rammeområda oppvekst, helse/omsorg og teknisk og arkiv. Personvernombodet har møterett og er rådgjevar for utvalet. ITU har følgjande hovudoppgåver:

- førebur leiinga si årlege gjennomgang av informasjonstryggleiken ut frå fastlagt rutine. I dette ligg også forslag til endringar og korrigerande tiltak.
- førebur tryggleiksrelaterte saker som skal til Rådmannen for informasjon eller avgjerd
- følgjer opp og tar avgjerd i saker der utvalet er delegert avgjerdsmynde
- handterer kritisk avviksrapportering som gjeld informasjonstryggleiken
- følgjer opp nasjonale og lokale føringar for å betra informasjonstryggleiken i kommunen

«IT-sjef»

- har delegert mynde til å ivareta rådmannen sitt overordna ansvar for planlegging, tryggleik, organisering, koordinering og styring av kommunen sin datatekniske infrastruktur.
- skal fastsetje minimumskrav til systemteknisk tryggleik på alle IKT- system som nyttar kommunen sitt datanett, og kontrollera at systemeigarar etterlever dette i praksis.
- skal gje råd til kommunen sine systemeigarar om systemteknisk tryggleik, tilrå løysingar i forhold til tryggleiksbehov
- skal konsulterast før nye system skal kjøpast inn og kontrollera at naudsynt tryggleik er ivaretatt før innkjøp. IT-sjef skal kontrollera at formalitetar mellom Vindafjord kommune og leverandørar er dokumentert i formelle kontraktar, og inkluderer relevante tryggleikskrav. Vindafjord kommune v/IT-sjef skal alltid ha rett til innsyn og måling av om leverandøren etterlever avtalte tryggleikskrav.
- skal kunna dokumentera kommunen sine IKT- system, og kunna presentere dette for eventuelle tilsyn.
- skal utarbeida rutine for oppretting, endring og avslutning av autorisasjonar .
- skal varsla om installasjonar og oppgraderingar, og i så stor grad som mogeleg leggja slikt arbeid til tider som gir med minst mogeleg ulempe for brukarane.

«Arkivleiar»

- har i tillegg delegert mynde til å ivareta rådmannen sitt overordna ansvar for planlegging av kommunal dokumenttryggleik knytt til arkivfunksjonar. Planleggingа skal omfatta arkivplanlegging, sikring, bevaring og lagring av dokumentasjon, både fysiske dokument og elektronisk materiale.
- skal gje råd om tryggleik og krav utifrå arkivlovgjevinga, og tilrå løysingar for å ivareta krava
- skal føre tilsyn med arkivlokale og arkivrom og sikre at desse er i forskiftsmessig stand både i høve til fysisk tryggleik og tilgangsrettar.

«Systemeigar»

Er den leiar som eig eit system eller ein applikasjon.
Vanlegvis er denne rolla tillagt ein einingsleiar eller kommunalsjef. Systemeigar har ansvar for;

- å konsultera IT-sjef og arkivleiar ved planlegging av innkjøp av nye system eller endringar i desse.
- å avklara at systemet tilfredsstiller overordna krav til informasjonstryggleik og bevarings-

tryggleik.

- at det er utarbeid rutinar for bruk, drift og vedlikehald av systemet. Ved rutineavvik er systemeigar ansvarleg for avvikshandtering og rapportering til informasjonstryggleiksutvalet (ITU)
- at systema blir brukt i samsvar med fastlagde rutinar
- at system som behandlar personopplysningar, sensitive personopplysningar, eller annan sensitiv informasjon har tilfredsstillande brukaradministrasjon og tilgangsstyring.
- Tryggleikskrava skal vera i samsvar med det tryggleiksnivå informasjonen krev.
- å sjå til at system som samkommuniserer har tilstrekkeleg tryggleik.
- å gjennomføra ei risikoanalyse ved alle større endringar/tilpassingar jf. Vedlegg risikovurdering.
- å halda systemadministratorar og IKT godt orienterte om planlagde endringar/ nyetableringar som vil koma.
- Å handtera ikkje-kritiske avvik.

«Systemansvarleg»

Er systemeigaren sin næraste medarbeidar i drift og vedlikehald av system eller applikasjon. Systemansvarleg har ansvar for

- at systemet blir sett opp med tilfredsstillande informasjonstryggleik, og syta for at lov og forskrifter blir følgd opp i systemet.
- å styra tilgangar og rettar etter rammer gitt av systemeigar, og rapporterer avvik og forbetringsforslag til systemeigar

Leiinga si gjennomgang

Leiinga si gjennomgang skal gjennomførast første halvår kvart år av strategisk leiargruppe. Den tryggleiksansvarlege legg til rette gjennomgangen og sørger for innspel og behandling i *Informasjonstryggleiksutvalet (ITU),* som tilrår til strategisk leiargruppe.

Gjennomgangen skal minst innehalde:

1. følgja opp dei mål som er sette
2. gjennomgang av avvik og hendingar
3. gjera korrigerande tiltak
4. vurdera oppfølging av korrigerande tiltak
5. endring av mål for prosess
6. sørge for at internkontroll og styringssystem for informasjonstryggleik er hensiktsmessig, tilstrekkeleg og effektivt og at det tilfredsstiller relevante krav i personvernregelverket
7. planar for vidare arbeid med informasjonstryggleiken

Gjennomgangen skal skje ut frå denne malen: Leiinga si gjennomgang (vedlegg)

I tillegg skal det vera eit møte mellom kommunen sine representantar i ITU og strategisk leiargruppe (kan kombinerast med leiinga si gjennomgang).

Gjennomførande dokumentasjon

Gjennomførande dokumentasjon beskriv de organisatoriske og tekniske tiltaka som er føreslått

som følge av at kommunen har vurdert *risiko* for rettar og fridomar, for eksempel tiltak for å ivareta ulike rettar for dei registrerte, tiltak for innebygd personvern, og tiltak for å oppnå tilstrekkeleg informasjonstryggleik.

Dokumentasjonen skal sikra at aktiviteten i kommunen samsvarar med kommunen sine definerte mål og retningslinjer for personvern og andre reglar. Denne dokumentasjonen skal også vera interne køyrereglar for dei tilsette, som sikrar at kommunen ikkje bryt lova med sine aktivitetar.

Beskriving av informasjonssystemet

Hovudpunkta i beskrivinga er arkitektur, grensesnitt ut av/inn til kommunen, intern ruter / IP-nett nettverkskomponentar, overvaking, logging og andre tryggleikstiltak.

Det ligg i tillegg ved eit eige konfigurasjonskart, som er sladda for innsyn for andre enn dei som er ansvarlege for at systemet er oppe å går til ei kvar tid.

Driftsrutinar

IKT har eige internkontrollsystem der berre IKT avdelinga har tilgang, der bl.a. følgjande rutinar er lagra:

- *Tryggleikskopiering*
- *Kundebehandling*
- *Saksbehandling*
- *Brukartilgangar*
- *Innkjøp*
- *Oppdateringar*
- *Nettverk*

Rutinar for testing av naudstraum er utarbeidde og blir følgd opp av kommunaltekniske tenester

Rutinar for handtering av personopplysningar er behandla som eit eige punkt.

Fysisk tryggleik

Beskrivinga gjeld kva fysiske område i kommunen og/eller heile bygningar som skal vernast som følge av behandling av personopplysningar, rutinar og tekniske tiltak for tilgangskontroll til slike verna område og tiltak for å verna mot innbrot, vasskade og brann.

Bygningar

Leiar av kvart resultatområde har ansvar for å utarbeida oversikt over utlevering og innlevering av tilgangskort/nøklar for sitt ansvarsområde. Det skal kvitterast skriftleg for utleverte og innleverte nøklar.

Personar som ikkje er autorisert som brukar av informasjonssystemet (besøkande), skal ikkje kunna gå fritt i lokale der det er plassert klientmaskinar som vert nytta til handsaming av sensitive personopplysningar.

Skrivarar

Fellesskrivarar skal berre brukast saman med personidentifikasjon og logging, og skal så langt råd plasserast på eigne rom/ekspedisjonar.
Unntak frå denne regelen er utskrifter i undervisningssamanheng /skrivarar på skulane.
Den som aktiviserer skrivaren for å skriva ut sensitive personopplysningar, plikter å sikre at alle dokument er tatt ut før ein går frå maskina. Dersom det oppstår feil, så skal feil meldast til maskinansvarleg, slik at ein sikrar at personsensitive opplysningar ikkje kjem på avvegar.

Kopiering

Brukar må vente ved kopimaskina til alle dokument med sensitive personopplysningar er ferdigkopierte. Den som kopierer, pliktar å sjå til at maskina er tømt for originalar og kopiar før han/ho forlét maskina.

Kontor

Dei fleste lokala kan vere opne for besøk i kontortida, men besøkande skal aldri vere åleine utan at pc er låst og der ikkje ligg framme dokument med skjerma innhald.
Kontor der det blir behandla sensitive personopplysningar, skal låsast når autorisert personell ikkje har tilsyn med rommet. Dokument med sensitive personopplysningar skal lagrast nedlåst etter kontortid.
Einskilde einingar (NAV, Barnevern ofl.) kan ha eigne og strengare reglar for tilgang. Einingsleiar pliktar å setja dei tilsette inn i desse rutinane.

Arkiv

- Daglegarkiv (arkivskap, rullereolar) skal låsast ved arbeidsdagens slutt, og når arkivet ikkje er under tilsyn i arbeidstida.
  På kontor der daglegarkiv består av permar i hyller skal kontor vera låst ved arbeidsdagens slutt, eller når kontorpersonale ikkje er til stades.
- Bortsetjingsarkiv på dei ulike einingane skal vera låst når der ikkje er personell til stades. Nøkkel skal oppbevarast av person med arkivansvar og/eller leiar.
- Sentralt bortsetjingsarkiv på rådhuset og på teknisk bygg skal vera låst med elektronisk låsesystem. Berre arkivpersonell og leiarar skal ha tilgang til desse romma og der skal førast tilgangsregister. Der skal førast logg over alle oppdrag i sentralt bortsetjingsarkiv.

Handtering av personopplysningar

Vindafjord kommune skal berre behandla nødvendige opplysningar om tilsette og brukarar. Dei som blir registrert, skal vera klar over at dette blir gjort. Dersom det er nødvendig, skal kommunen be om heimel til det.

Vindafjord kommune skal kunna svara på spørsmål, både frå registrerte og publikum generelt, om korleis me behandlar personopplysningar.

Kommunen brukar systemet for tida programmet *Draftit* til protokollføring og å halda oversikt over kva system behandling av personopplysningar skjer i. Protokollen inkluderer blant anna oversikt over type behandlingsaktivitetar, kategoriar av personopplysningar og registrerte, rettsleg grunnlag og formål med behandlingane.

I systemet er det også registrert kva *databehandlaravtalar* kommunen har med sine underleverandørar (artikkel 28 og 29). Databehandlaravtalen skal sikra at personopplysningar blir behandla i samsvar med regelverket og set ei klar ramme for korleis databehandlaren kan behandla opplysningar. Databehandlaravtalane skal arkiverast i Websak.
Protokollen inngår i styringsdokument for internkontroll og skal gjennomgåast og oppdaterast jamleg.

Risikovurdering

Ut frå kva potensiale dei ulike systema representerer i forhold til konsekvens, gjer me ein overordna vurdering av kva vernebehov som er nødvendig. System kor katastrofale hendingar kan inntreffa vil normalt, uavhengig av sannsynlegheit, ha behov for en betre vern enn system kor slike hendingar ikkje kan inntreffa.

Me vurderer først kva sikkerheitsaspekt som er relevante for hendinga (konfidensialitet, integritet, tilgjengelegheit og/eller robustheit - KITR). Så blir det gitt ein vurdering av mogleg konsekvens, sannsynlegheit for at hendinga skal inntreffa og risiko som følgje av dette. Til slutt blir det gitt ein vurdering av om risikoen er akseptabel eller ikkje.

Kommunen har gjennomført ROS-analysar for ei rekke grupper av behandlingar i samband med registrering i Draftit. Dokumentasjon på desse ligg i Draftit.

Vurdering av personvernkonsekvensar (DPIA)

Dersom det er sannsynleg at ein type behandling, *særleg ved bruk av ny teknologi* og når det tas omsyn til behandlingas art, omfang, formål og samanhengen den blir utført i, vil medføre *ein høg risiko* for fysiske personar sine rettar og fridomar, skal den behandlingsansvarlege *før behandlinga* foreta ei vurdering av *kva konsekvensar* den planlagde behandlinga vil ha for vernet av personopplysningar (artikkel 35 nr. 1).

Datatilsynet har laga denne lista, som er godkjent av det europeiske personvernrådet (2019), over behandlingsaktivitetar som alltid krev at det blir gjennomført DPIA:

1. Personopplysningar samla inn via ein tredjepart i følgje med minst eitt anna kriterium.
2. Behandling av biometriske opplysningar for å identifisera enkeltpersonar i følgje med minst eitt anna kriterium.
3. Behandling av genetiske opplysningar i følgje med minst eitt anna kriterium.
4. *Behandling av personopplysningar* med innovativ teknologi i følgje med minst eitt anna kriterium.
5. Behandling av personopplysningar for systematisk monitorering av tilsette.
6. Behandling av personopplysningar, utan *samtykke*, for vitskapelege eller historiske formål i følgje med minst eitt anna kriterium.
7. Behandling av lokasjonsdata i følgje med minst eitt anna kriterium.
8. Behandling av personopplysningar for å evaluera læring, meistring og trivsel i skular eller barnehagar.
   Dette inkluderer alle utdanningsnivå, frå barne- og ungdomsskule, vidaregåande skular og høgare utdanning. (Sårbare registrerte og systematisk monitorering.)
9. Systematisk monitorering, inkludert kameraovervaking, på offentleg tilgjengelege område i stor skala. (Systematisk monitorering og stor skala.)

10. Kameraovervaking i skular og barnehagar i opningstider. (Systematisk monitorering og sårbare registrerte)
11. Behandling av særlige kategoriar av personopplysningar eller svært personlege opplysningar i stor skala for algoritmetrening.
12. Behandling av personopplysningar ved å systematisk monitorera effektivitet, ferdigheiter, kunnskap, mental helse og utvikling. (Svært personlege opplysningar og systematisk monitorering).
13. Behandling av personopplysningar der formålet er å tilby ei teneste eller utvikla produkt for kommersiell bruk som involverer å føreseie jobbprestasjonar, økonomi, helse, personlege preferansar eller interesser, pålitelegheit, åtferd, lokasjon eller bevegelsesmønster. (Særlege kategoriar av personopplysningar eller svært personlege opplysningar og evaluering/poengsetjing).
14. Innsamling av personopplysningar i stor skala gjennom «tingenes internett (IOT)» eller velferdsteknologi. (Stor skala og særlege kategoriar av opplysningar eller svært personlege opplysningar

I tillegg har Datatilsynet laga denne lista over behandlingar som ikkje krev at det blir gjennomført DPIA:

1. Dersom behandlinga sannsynlegvis ikkje «vil medføra ein høg risiko».
2. Dersom behandlingas art, omfang, samanheng og formål er veldig lik ei behandling det allereie er gjennomført ei vurdering av personvernkonsekvensar for. I slike situasjonar kan resultatet frå den føreliggjande vurderinga for liknande behandlingar brukast.
3. Dersom behandlinga er kontrollert av ein tilsynsmyndigheit før mai 2018 på særskilte vilkår, og at desse ikkje har endra seg. (I Noreg vil ein slik kontroll vanlegvis bety at ein har hatt *konsesjon*).
4. Dersom ei behandling er i samsvar med artikkel 6 nr. 1 bokstav c (rettsleg plikt) eller bokstav e (utføre ei oppgåve i ålmentas interesse eller utøva offentleg mynde) **og** har eit rettsgrunnlag etter EU-retten eller nasjonal lovgiving, der tilhøyrande lovgiving regulerer den spesifikke behandlinga og ei vurdering av personvernkonsekvensar allereie er gjennomført som ledd i utarbeiding av rettsgrunnlaget (artikkel 35 nr. 10), unntatt viss medlemsstaten har bestemt at det er nødvendig å gjennomføra ei vurdering av personvernkonsekvensar forut for behandlinga.

For gjennomføring av DPIA blir det vist til rettleiaren som Datatilsynet har utarbeidd og er å finne på Datatilsynet sine sider.

Innsyn og endring/sletting i eigne opplysningar

Hovudprinsippet er at alle har rett til å bestemme over eigne personopplysningar. Retten til innsyn i eigne personopplysningar og informasjonsplikta når det samlast inn personopplysningar er beskrive i artikkel 15 i personopplysningslova. Retten til å få opplysningane sine retta er beskrive i artikkel 16, og retten til å få opplysningane sine sletta er beskrive i artikkel 17. Arkivlov og faglovene om journalføring har eigne bestemmingar om dette, som gjeld føre personvernforordninga.

Ved tvil om personen har krav på innsyn, informasjon om innsamling av personopplysningar, eller å få retta eller sletta personopplysningar, skal

personvernombodet kontaktast.

Det er behandlingsansvarleg som har ansvaret for at rutinane for mottak og behandling av førespurnadar som dreiar seg om innsyn etter personvernforordninga blir varetatt. Behandlingsansvarleg kan delegere ansvaret for den praktiske gjennomføringa til aktuell saksbehandlar.

Innsyn etter forvaltningslova §§18-21 følgjer andre rutinar og må vurderast særskilt.

Informasjonsplikta ved innsamling av personopplysningar

Mottak av opplysningar

Ved mottak av personopplysningar frå personen sjølv eller frå andre system, skal behandlingsansvarleg sjekka om personen har krav på varsel om at det blir samla inn personopplysningar om han/ho.

Varsel om innsamling av personopplysningar

Dersom personen har krav på varsel skal behandlingsansvarleg oppgi formålet med behandlinga og sin kontaktinformasjon. Dette kan gjerast anten på e-post eller i sikker sending. Dersom opplysningane vil bli utlevert skal det oppgiast kven som mottar opplysninga. Det skal opplysast om at det er frivillig å gi frå seg opplysningane.
Sjå Datatilsynet sin rettleiar om «Informasjon og åpenhet»

Behandling av innsyn i eigne opplysningar

Alle kan be om innsyn i eigne personopplysningar anten skriftleg eller munnleg. Førespurnaden skal journalførast på arkivkode for personvernrettar og fordelast til ansvarleg leiar, som eventuelt delegerer vidare til saksbehandlar. ITU skal utarbeida forslag til rutinar for behandling av innsyn av personopplysningar, som skal godkjennast av rådmannen.

Eksempel på innhald i slike rutinar kan vera:

- Iverksetjing eller opphøyr av behandling
- Informasjon
- Innhenting og kontroll av samtykke
- Innsyn i eigne personopplysningar
- Dataportabilitet
- Retting av personopplysningar
- Sletting av personopplysningar
- Avgrensing av behandling av personopplysningar
- Handtering av protestar og varetaking av retten til å protestera på behandling av personopplysningar
- Handtering av rettar ved automatiserte avgjersler
- Utlevering av personopplysningar til andre
- Overføring til tredjestatar

Nytilsette og tilsette som sluttar

Næraste leiar har ansvar for at tryggleiksaspektet blir følgd opp for nytilsette og tilsette som sluttar. Det er naturleg at dette blir tatt inn i introduksjonsprogrammet for nytilsette og i forbindelse med sluttsamtalen for tilsette som sluttar i kommunen. Det er utarbeidd sjekkliste for nytilsette og tilsette som sluttar.

Tryggleiksinstruksar

Det er utarbeidd tryggleiksintruks for tilsette (sjå vedlegg).

Gjennomførande dokumentasjon bør også byggast på med ei overordna beredskapsplan for informasjonstryggleik.

Kontrollerande dokumentasjon

Kontrollerande dokumentasjon er dokument som har til formål å verifisere at aktivitetane har føregått i samsvar med fastsette rutinar og instruksar. Eksempel er rapportar, sjekklister og logg. Kontrollerande dokumentasjon kan sjåast på som eit «sikringsnett» som bidreg til at styringsdokumenta blir følgde og at eventuelle *avvik* lettare blir oppdaga. Dokumenta skal ikkje vera statiske, men endra seg i tråd med utviklinga i kommunen og den rettslege utviklinga.

Det er eit klart skilje mellom gjennomførande og kontrollerande dokumentasjon. Det første skal sikra at aktivitetane er i samsvar med mål og retningslinjer. Det siste skal bidra til at avvik frå mål og retningslinjer blir oppdaga og retta.

Avvik

Avviksbehandling blir sett i verk ved tryggleiksbrot og/eller når oppgåver er utført i strid med rutinar som er vedtatt. Behandling av dei uønskte hendingane i informasjonssystemet har til formål å gjenoppretta normal tilstand og å hindra at hendinga gjentar seg.

Avviksbehandling vil normalt omfatta rapportering, strakstiltak, permanent korrigering av avvik og oppfølging av korrigerande tiltak over tid for å vurdera om dei fungerer etter formålet sitt.

Ved brot på personopplysningstryggleiken skal den behandlingsansvarlege utan ugrunna opphald og når det er mogleg, seinast 72 timer etter å ha fått kjennskap til det, melda brotet til Datatilsynet, med mindre brotet sannsynlegvis ikkje vil medføra ein risiko for fysiske personar sine rettar og fridomar. Dersom brotet ikkje blir meldt til tilsynsmyndigheita innan 72 timer, skal årsakene til forseinkinga oppgiast.

- Personvernforordninga artikkel 33 nr. 1

Dersom det er sannsynleg at brotet på personopplysningstryggleiken vil medføra høy risiko for fysiske personar sine rettar og fridomar, skal den behandlingsansvarlege utan ugrunna opphald underretta den registrerte om brotet.

- Personvernforordninga artikkel 34 nr. 1

Med ein gong ein blir klar over at det er har skjedd et brot, skal ein handtera og avgrensa det, men ein må samtidig avgjera kva risiko det kan ha medført for dei som er omfatta av brotet.

- Dersom det er ingen eller låg risiko, er det *ikkje behov* for å melda frå til Datatilsynet eller til dei som er omfatta.
- Dersom det er middels risiko, er det *nødvendig å melda* frå til Datatilsynet, men *ikkje informera dei som er omfatta*.
- Dersom det er høg risiko, er det *nødvendig å melda* frå til Datatilsynet *og informera* dei som er omfatta.

Når ein skal vurdera risiko av eit brot, må ein sjå på kor alvorleg brotet er og kva verknader det kan få?

Kva slags type brot er det?
Er det eit brot på:

- Konfidensialitet (K)
- integritet (I)
- tilgjengelegheit (T)
- robustheit (R)

Deretter vurderer ein konsekvensane av brotet opp mot (KITR) .

Avvik skal alltid handterast internt. Dersom det ikkje blir meldt til Datatilsynet eller at dei som er omfatta ikkje blir varsla, skal det grunngiast i ein *intern avviksrapport* for kommunen.

Rapportering av avvik skal starta hos den medarbeidaren som oppdagar avviket. Avvik skal som hovudregel meldast i kommunen sitt avvikssystem.

Systemteknisk avvikshandsaming og korrigerande tekniske tiltak vert gjort av It-driftsansvarleg.

Andre korrigerande tiltak vert gjort av leiaren i eininga som avviket gjeld.

Ei avviksbehandling er sett saman av:

- *Avdekking av avviket*
- *Rapportering; dette vert normalt utført av den medarbeidaren som oppdagar avviket. Avviket blir rapportert til personvernombod, tryggleiksansvarleg og ansvarleg i linjeorganisasjonen*
- *Vurdera melding til Datatilsynet og varsling til dei som er omfatta.*
- *Iverksetjing av strakstiltak mellom anna med det formålet å avgrensa eventuelle følgjeskadar. Strakstiltaka kan utførast av den medarbeidaren som oppdagar avviket, eventuelt av den medarbeidaren som har ansvar for den delen av informasjonssystemet avviket gjeld.*
- *Iverksetjing av korrigerande tiltak for permanent å igjen oppretta normal tilstand. It-driftsansvarleg eller ansvarleg i linjeorganisasjonen syt for at dette skjer.*
- *Vurdering (etter ei tid) om korrigerande tiltak fungerer slik det var meinte. Vurderinga vert utført av It-driftsansvarleg, ansvarleg i linjeorganisasjonen eller eventuelt av tryggleiksansvarleg ved gjennomføring av internkontroll.*

Tryggleiksrevisjon/Eigenkontroll

Den behandlingsansvarlege skal med jamne mellomrom, minimum ein gong pr. år, etterprøva tryggleiken for å verifisera at dei tryggleikstiltaka som er vedtatt etablert, er sett i verk og fungerer etter formålet. Ved tryggleiksrevisjon vert den faktiske bruken av informasjonssystemet samanlikna med dei retningslinene for bruk som er vedtatt. Resultatet av tryggleiksrevisjonen vil vera ein del av grunnlaget for leiinga si gjennomgang og må vera gjennomført i forkant.

Denne revisjonen må ikkje blandast saman med leiinga si gjennomgang av tryggleiksmål og strategi, der formålet er å vurdera leiinga sine vedtak opp mot verksemda si trong for informasjonsteknologi og informasjonstryggleik.

Tryggleiksrevisjon er eit viktig grunnlag for kontinuerleg forbetring av informasjonstryggleiken.

Definisjonar og forklaringar

Avvik	Hending eller situasjon som bryt med gjeldande reglar.
Informasjonstryggleik	Sikring av opplysningar ved å bruke prinsippa om konfidensialitet, integritet og tilgjenge.
Konfidensialitet	Prinsipp om at personopplysningar må vera sikra mot at uvedkommande får tilgang til dei.
Integritet	Prinsipp om at personopplysningar skal vera sikra mot utilsikta eller ikkje autorisert endring eller sletting.
Tilgjenge	Prinsippet om at personopplysningar skal vera tilgjengelege for det formålet dei er tiltenkt.
Personopplysning	Opplysning eller vurdering som kan knytast til ein enkeltperson. Dette kan vera namn, adresse, telefonnummer, e-postadresse, bilnummer, bilete eller fødselsdato.
Personregister	Systematisk samling av personopplysningar.
Behandling av personopplysningar	All bruk av personopplysningar, slik som innsamling, registrering, samanstilling, lagring og utlevering, eller ein kombinasjon av slike bruksmåtar.
Behandlingsgrunnlag	Rettsleg grunnlag for å behandla personopplysningar. Dette kan for eksempel vera samtykke.
Behandlingsansvarleg	Den som bestemmer formålet med behandlinga av personopplysningar og kva hjelpemidlar som skal brukast. Dette er vanlegvis ei verksemd. Rådmannen utøver behandlingsansvaret for kommunen.
Databehandlar	Den som behandlar personopplysningar på oppdrag frå den behandlingsansvarlege. Dette er vanlegvis ei verksemd.
Registrert	Enkeltpersonen som dei lagra opplysningane kan knytast til.
Samtykke	Ei frivillig, spesifikk, informert, heilt tydeleg og aktiv erklæring frå den registrerte om at han eller hun godtar behandling av opplysningar om seg sjølv. Eit samtykke kan trekkast tilbake når som helst utan negative konsekvensar. Verksemder må kunne dokumentera at samtykke er gitt.
Sensitive	I lova kalla særskilte kategoriar av personopplysningar.

personopplysningar	Opplysningskategoriane dette gjeld er: 1. opplysningar om rase eller etnisk bakgrunn 2. opplysningar om politisk oppfatning 3. opplysningar om religion 4. opplysningar om filosofisk overtyding 5. opplysningar om fagforeiningsmedlemskap 6. genetiske opplysningar 7. biometriske opplysningar med det formål å eintydig identifisera nokon 8. helseopplysningar 9. opplysningar om seksuelle forhold 10. opplysningar om seksuell legning 11. opplysningar om straffedommar 12. opplysningar om lovbrot
Tryggleiksansvarleg	Den eller dei personar innan kommunen sin administrasjon som har ansvar for tryggleik, deriblant datatryggleiken kommunen. Ansvaret ligg inntil vidare hos kommunalsjefane, økonomisjef og personal- og organisasjonssjef.
IT sjef	Den person som har fått delegert rådmannen sitt overordna ansvar for for planlegging, tryggleik, organisering, koordinering og styring av kommunen sin datatekniske infrastruktur.
Systemeigar	Er den leiar som eig eit system eller ein applikasjon. Vanlegvis er denne rolla tillagt ein einingsleiar eller kommunalsjef
Systemansvarleg	Er systemeigaren sin næraste medarbeidar i drift og vedlikehald av system eller applikasjon.

Vidare arbeid:

Innafor tidsramma for arbeidet med dette dokumentet, har det ikkje vore høve til å avklare alle forhold som er nødvendige. Dette gjeld avklaringar med eksterne samarbeidspartnarar og prosessar med utarbeiding av rutinar, der eit godt resultat er avhengig av breiare intern medverknad. Dette gjeld m.a.:

- *Avklara felles personvernombod*
- *Avklara stilling/funksjon som tryggleiksansvarleg*
- *Leggja til rette for avviksbehandling i kommunen sitt kvalitetssystem*
- *Utarbeiding av manglande rutinar som beskrive i dokumentet*
- *Utarbeida evt. manglande delegasjonar*
- *Avklara ITU sine oppgåver og ansvarsområde*
- *Generell kompetanseheving på området som del av opplæringsplan*
- *Vurdera utarbeiding av overordna beredskapsplan for informasjonssystema*

Vedlegg:

- *Leiinga si gjennomgang*
- *Rammer for risikovurdering*
- *Verktøy risikovurdering rekneark*
- *Sjekkliste for nytilsette og tilsette som sluttar*
- *Avvikshandtering*
- *Avviksskjema-internt*
- *Beskriving av informasjonssystemet med sladda konfigurasjonskart (Vindafjord Lag 3 anonymisert (002))*

Dokument under utarbeiding (leggast ved endeleg dokument):

- *Tryggleiksinstruks brukar*

Eksempel på malar til bruk ved utarbeiding av andre instruksar/rutinar/skjema:

- *Informasjonshandtering oversyn (evt. vedlegg til tryggleiksinstruks)*
- *Tryggleiksinstruks-leiar*
- *Tryggleiksrevisjon---eigenkontroll*
- *Eigenkontrollskjema*
- *Rutinar for handtering av personopplysningar*
- *Overordnet beredskapsplan for informasjonssystemer (bokmålsversjon)*