Forvaltningsrevisjon
Februar 2021

Personvern

Drammen kommune

Viken
kommunerevisjon

Sammendrag

Bestilling

Kontrollutvalget
sak 41/20
21. april 2020

Formål

Vurdere i hvilken grad kommunen har gjennomført de nødvendige steg som er pålagt for å kunne være i stand til å sikre et tilfredsstillende vern av fysiske personer i forbindelse med behandling av personopplysninger.

Problemstillinger

- **Har kommunen gjennomført risiko- og sårbarhetsanalyser (ROS)?**
- **Har kommunen tilpasset rutiner og retningslinjer?**
- **Har kommunen oppdaterte «databehandleravtaler»?**
- **Har kommunen foretatt nødvendige endringer på IKT?**
- **Har kommunen et personvernombud med en rolle som er i tråd med regelverket?**

Metode og praktisk gjennomføring

Prosjektet er gjennomført av revisjonens egne ansatte på bakgrunn av kravene som stilles til gjennomføring av forvaltningsrevisjon som prosjekt i *"RSK001 Standard for forvaltningsrevisjon"*.

Informasjonen som er presentert i dette prosjektet, er hentet inn gjennom dokumentanalyse og samtaler med nøkkelpersoner i kommunen.

I gjennomføringen har vi hatt dialog med personvernombudet, kommunens internkontroller og informasjonssikkerhetsansvarlig i virksomhet IKT. Vi har også hatt en samtale med personvernombudet med særlig fokus på personvernombudets rolle og arbeidsforhold i kommunen, sett opp mot problemstillingene som belyses i rapporten.

Revisjonskriterier

Som kilder for revisjonskriteriene har vi i hovedsak benyttet kommuneloven, personopplysningsloven og personopplysningsforskriften som er utarbeidet på bakgrunn av den nye personvernforordningen for EU/EØS. Vi har også benyttet utvalgte veiledere fra Datatilsynet. I kapittel 3 fremgår de utledede revisjonskriteriene til problemstillingene, og i vedlegg 4 fremgår selve utledningen av disse.

Oppsummering og konklusjoner

Drammen kommune har i dag en positiv utvikling i sitt personvernarbeid, og rutiner, retningslinjer og maler bidrar til et mer uniformt arbeid i hele kommunen. Dette vises gjennom risiko- og sårbarhetsanalyser og gjennomførte vurdering av personvernkonsekvenser (Data Protection Impact Assessment – DPIA). Det samme så vi også i databehandleravtaler, hvor det tidligere var mangler i hvilke databehandleravtaler man brukte og utfyllingen av disse.

Et fellestrekk vi har sett i gjennomgangen av Drammen kommunes personvernarbeid, er at det i dag eksisterer mangler som stammer fra tidligere og at det vil kreve ressurser for å sikre at dette arbeidet kommer à jour. Mye av dette arbeidet ser ut til å være avhengig av personvernombudet. Ikke fordi det pålegges, men fordi personvernombudet har sett at andre ikke tar tak i det. Et eksempel er

behandlingsprotokollen, en lovpålagt protokoll som Drammen kommune ennå ikke har utarbeidet en fullverdig versjon av.

Tilgjengelig dokumentasjon gir inntrykk av at kommunen ikke har noen strukturert oversikt over behovet for tilpasninger / endringer på IKT-systemer for å tilfredsstille personvernlovgivningen, eller hvilken status det er på dette arbeidet. Kommunen har gode maler for analyser og vurderinger på personvernområdet, men det er mangler i gjennomføringen for store deler av personvernområdet. Heller ikke her kan vi finne noe oversikt over status med dette arbeidet. Vi mener derfor at kommunen må prioritere arbeidet med å sikre at kartlegginger er eller blir gjennomført, samt utarbeide en oversikt over oppfølging av de tiltak som disse medfører.

Kommunesammenslåingen hvor tre kommuner ble en, samt en IKT-virksomhet som lå «på siden» av kommunen og nå er en del av kommunens basisorganisasjon virker å ha gitt mange utfordringer på IKT-området. Blant annet i forbindelse med alt arbeidet som er lagt ned i valg av systemer, endringer og tilpasninger, justering av brukeradferd, ROS-analyser, informasjonssikkerhet og personvern. I denne «kampen» om fokus og prioritering virker det på oss som om personvern og personvernombudet ikke har nådd så høyt opp på prioriteringslisten som hadde vært ønskelig.

Anbefalinger

Med bakgrunn i vår gjennomgang vil vi anbefale kommunedirektøren / Drammen kommune å gjennomføre følgende:

- **Sørge for tilstrekkelige ressurser for å sikre at protokoller over behandlingsaktiviteter fullføres.**
- **Sikre at det utarbeides en sentral oversikt (system) for å holde oversikt over kartlegging av behov for nødvendige endringer på IKT og status på tiltak som disse medfører**
- **Sikre at kompetansen og forståelsen om personvernlovgivningen er tilstrekkelig i egen virksomhet.**
- **Vurdere å endre rapporteringsnivået for personvernombudet fra nivå 2 til nivå 1.**

Et utkast til rapport har blitt oversendt kommunedirektøren til uttalelse. Kommunedirektørens uttalelse i brev av 19. februar 2021 er vedlagt rapporten.

Innhold

1. Innledning

1.1. Bakgrunn for prosjektet

Kontrollutvalget i Drammen kommune vedtok i sitt møte 21. april 2020, sak 41/20, at Viken kommunerevisjon IKS (VKR) skulle gjennomføre en forvaltningsrevisjon av innenfor området personvern.

Prosjektet er bestilt på bakgrunn av drøftinger i kontrollutvalget i Drammen kommune den 13. februar 2020. Prosjektet er aktuelt på bakgrunn av det fokus som har vært på området i forbindelse med den nye forordningen[1] som ble vedtatt i EU 27. april 2016, og senere ble tatt inn som norsk lov gjennom den nye personopplysningsloven[2] som fikk trådte i kraft fra 25. august 2018.

Regelverket som ble innført gjennom den nye personvernforordningen og personopplysningsloven gjelder ved helt eller delvis automatisert behandling av personopplysninger, og ved ikke-automatisert behandling av personopplysninger som inngår i eller skal inngå i et register. Dette innebærer at det ofte vil omhandle elektronisk behandling (IKT) av personopplysninger, men at det også i gitte tilfeller vil omfatte manuell behandling (papir).

Det nye regelverket krever mer åpenhet rundt innsamling og bruk av personopplysninger. Den som ber om samtykke til å bruke opplysninger skal gi klar og tydelig informasjon om hvordan personopplysningene skal brukes. Bruken av personopplysninger skal begrunnes og begrenses, og det er ikke være lov å samle inn eller lagre personopplysninger man ikke trenger. Når det ikke lenger er behov for opplysningene, skal de slettes.

Den registrerte har også rett til at uriktige eller ufullstendige opplysninger skal rettes. Den har videre rett til å ta med seg personopplysninger fra en virksomhet til en annen. Den registrerte har også rett til å protestere mot behandling av sine personopplysninger, og kan slippe at det blir truffet viktige avgjørelser om ham eller henne basert på en helautomatisert behandling av personopplysninger.

Det nye regelverket åpner også for å ilegge et betydelig høyere gebyr ved overtredelse av reglene enn det var rom for i det gamle regelverket.

Det er derfor viktig at kommunen har oversikt over hvilke systemer som behandler personopplysninger, hvordan informasjonsutveksling (integrasjon) mellom systemene er og hvilke opplysninger som (skal) oppbevares og hvor lenge. Det siste punktet innebærer også at kommunen må ha oversikt over, og et systematisk forhold til hva og når aktuelle personopplysninger skal slettes.

[1] EUROPAPARLAMENTS- OG RÅDSFORORDNING (EU) 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt om oppheving av direktiv 95/46/EF (generell personvernforordning)
[2] LOV 2018-06-15 nr 38, Lov om behandling av personopplysninger (personopplysningsloven)

1.2. Formål og problemstillinger

Prosjektets formål er å vurdere om Drammen kommune har gjennomført de nødvendige steg som er pålagt for å kunne være i stand til å sikre et tilfredsstillende vern av fysiske personer i forbindelse med behandling av personopplysninger.

I denne forvaltningsrevisjonen søker vi å belyse følgende problemstillinger:

- **Har kommunen gjennomført risiko- og sårbarhetsanalyser (ROS)?**
- **Har kommunen tilpasset rutiner og retningslinjer?**
- **Har kommunen oppdaterte «databehandleravtaler»?**
- **Har kommunen foretatt nødvendige endringer på IKT?**
- **Har kommunen et personvernombud med en rolle som er i tråd med regelverket?**

1.3. Avgrensning av undersøkelsen

Som det går fram av problemstillingene i kulepunktene i kapittel 1.2, er det vedtatt relativt konkrete problemstillinger for forvaltningsrevisjonen. Vi presiserer at prosjektet kun tar for seg de områder og temaer som faller inn under de problemstillingene som fremgår av kapittel 1.2. Vurderinger og konklusjoner omfatter derfor bare disse avgrensede definerte områdene eller temaene.

Det er med andre ord ikke tale om en fullstendig gjennomgang av hvordan Drammen kommune håndterer personvern i alle sine administrative og faglige systemer og rutiner.

1.4. Definisjoner

Artikkel 4 i EUs personvernforordning[3] inneholder definisjon av sentrale begreper. Vi presenterer her noen sentrale begreper, og viser til vedlegg 5 for utdrag av hele Artikkel 4. En ordliste finnes også på Datatilsynets nettside[4].

Personopplysninger

> **enhver opplysning om en identifisert eller identifiserbar fysisk person («**den registrerte**»); en identifiserbar fysisk person er en person som direkte eller indirekte kan identifiseres, særlig ved hjelp av en identifikator, f.eks. et navn, et identifikasjonsnummer, lokaliseringsopplysninger, en nettidentifikator eller ett eller flere elementer som er spesifikke for nevnte fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sosiale identitet,**

[3] EUROPAPARLAMENTS- OG RÅDSFORORDNING (EU) 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt om oppheving av direktiv 95/46/EF (generell personvernforordning)

[4] https://www.datatilsynet.no/regelverk-og-verktoy/ordliste/

Behandling

enhver operasjon eller rekke av operasjoner som gjøres med personopplysninger, enten automatisert eller ikke, f.eks. innsamling, registrering, organisering, strukturering, lagring, tilpasning eller endring, gjenfinning, konsultering, bruk, utlevering ved overføring, spredning eller alle andre former for tilgjengeliggjøring, sammenstilling eller samkjøring, begrensning, sletting eller tilintetgjøring,

Register

enhver strukturert samling av personopplysninger som er tilgjengelig etter særlige kriterier, enten samlingen er plassert sentralt, er desentralisert eller spredt på et funksjonelt eller geografisk grunnlag,

Behandlingsansvarlig

en fysisk eller juridisk person, en offentlig myndighet, en institusjon eller ethvert annet organ som alene eller sammen med andre bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes; når formålet med og midlene for behandlingen er fastsatt i unionsretten eller i medlemsstatenes nasjonale rett, kan den behandlingsansvarlige, eller de særlige kriteriene for utpeking av vedkommende, fastsettes i unionsretten eller i medlemsstatenes nasjonale rett,

Databehandler

en fysisk eller juridisk person, offentlig myndighet, institusjon eller ethvert annet organ som behandler personopplysninger på vegne av den behandlingsansvarlige,

Mottaker

en fysisk eller juridisk person, offentlig myndighet, institusjon eller ethvert annet organ som personopplysninger utleveres til, enten det dreier seg om en tredjepart eller ikke. Offentlige myndigheter som kan motta personopplysninger innenfor rammen av en særskilt undersøkelse i samsvar med unionsretten eller medlemsstatenes nasjonale rett, skal imidlertid ikke anses som mottakere; nevnte offentlige myndigheters behandling av slike opplysninger skal være i samsvar med gjeldende regler om vern av personopplysninger i henhold til formålet med behandlingen,

Tredjepart

enhver annen fysisk eller juridisk person, offentlig myndighet, institusjon eller ethvert annet organ enn den registrerte, den behandlingsansvarlige, databehandleren og de personer som under den behandlingsansvarlige eller databehandlerens direkte myndighet har fullmakt til å behandle personopplysninger,

Samtykke

fra den registrerte 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,

2. Metode

Prosjektet er gjennomført av revisjonens egne ansatte på bakgrunn av kravene som stilles til gjennomføring av forvaltningsrevisjon som prosjekt. Det vil si at gjennomgangen er basert på *"RSK 001 Standard for forvaltningsrevisjon"*[5] som er vedtatt av Norges Kommunerevisorforbund (NKRF).

Informasjonen som er presentert i dette prosjektet, er hentet inn gjennom dokumentanalyse og samtaler med nøkkelpersoner i kommunen.

I gjennomføringen har vi hatt dialog med personvernombudet, kommunens internkontroller og informasjonssikkerhetsansvarlig i virksomhet IKT. Vi har også hatt en samtale med personvernombudet med særlig fokus på personvernombudets rolle og arbeidsforhold i kommunen, sett opp mot problemstillingene som belyses i rapporten.

Vi mener det er samlet inn et tilstrekkelig faktagrunnlag til å belyse problemstillingene og revisjonskriteriene.

Vi viser kapittel 1.3 for eventuelle avgrensinger i prosjektets omfang.

Et utkast til rapport har blitt oversendt kommunedirektøren til uttalelse. Kommunedirektørens uttalelse i brev av 19. februar 2021 er vedlagt rapporten.

For ytterligere beskrivelse av metode, se vedlegg[6].

[5] Vedlegg 2 – RSK 001 – Standard for forvaltningsrevisjon
[6] Vedlegg 3 – Metode

3. Revisjonskriterier

Som kilder for revisjonskriteriene[7] har vi i hovedsak benyttet kommuneloven[8], personopplysningsloven[9] og personopplysningsforskriften[10] som er utarbeidet på bakgrunn av den nye personvernforordningen for EU/EØS[11]. Vi har også benyttet utvalgte veiledere fra Datatilsynet[12].

På bakgrunn av problemstillingene og relevante krav i kildene[13], har vi utledet følgende revisjonskriterier for vår gjennomgang av personvern i Drammen kommune. Kriteriene er ikke nødvendigvis uttømmende for ethvert krav som stilles til alle sider av arbeidet innenfor personvern i Drammen kommune. Kriteriene er oppstilt etter revisjonens vurdering av hva som er det sentrale, basert på en vurdering av virksomhetens egenart og regelverket den forvalter.

Risiko- og sårbarhetsanalyser (ROS)

Den første problemstillingen er:

- ***Har kommunen gjennomført risiko- og sårbarhetsanalyser (ROS)?***

Utledede revisjonskriterier:

- ***Kommunen skal gi en vurdering av personvernkonsekvenser***
- ***Kommunen skal føre protokoller over behandlingsaktiviteter***
- ***Kommunen skal gi en vurdering av risikoene for de registrertes rettigheter og friheter***
- ***Kommunen skal gi en vurdering av de planlagte tiltakene for å håndtere risikoene, herunder garantier, sikkerhetstiltak og mekanismer for å sikre vern av personopplysningen***

---

[7] Revisjonskriterier er en samlebetegnelse for krav og forventninger som benyttes for å vurdere kommunens virksomhet, økonomi, produktivitet, måloppnåelse, regeletterlevelse osv. Sammenholdt med faktabeskrivelsen danner revisjonskriteriene basis for de analyser og vurderinger som foretas, de konklusjoner som trekkes, og de er et viktig grunnlag for å kunne dokumentere avvik eller svakheter.
[8] LOV 1992-09-25 nr 107 – Lov om kommuner og fylkeskommuner (kommuneloven)
Erstattet av: LOV 2018-06-22 nr 83 – Lov om kommuner og fylkeskommuner (kommuneloven)
I kraft fra og med det konstituerende møtet i det enkelte kommunestyret og fylkestinget ved oppstart av valgperioden 2019-2023
[9] LOV 2018-12-20 nr 116, Lov om behandling av personopplysninger (personopplysningsloven)
[10] FOR 2018-06-15 nr 876, Forskrift om behandling av personopplysninger
[11] EUROPAPARLAMENTS- OG RÅDSFORORDNING (EU) 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt om oppheving av direktiv 95/46/EF (generell personvernforordning)
[12] Oversikt over veiledere fra Datatilsynet som er benyttet finnes i "Referanser" bak i rapporten.
[13] Vedlegg 4 – Utledning av revisjonskriterier

Tilpassede rutiner og retningslinjer

Den andre problemstillingen er:

- ***Har kommunen tilpasset rutiner og retningslinjer?***

Utledede revisjonskriterier:

- ***Kommunen skal ha et formål med behandling av personopplysninger, og gjennom dette rutiner for å identifisere om det finnes behandlingsgrunnlag***
- ***Kommunen skal innhente samtykke der det ikke foreligger annen hjemmel for behandling***
- ***Kommunen skal utarbeide personvernerklæring hvor informasjonen er kortfattet, åpen, forståelig og lett tilgjengelig***
- ***Kommunen skal ha rutiner for sletting av personopplysninger som ikke lengre er nødvendige for formålet de ble samlet inn for***
- ***Kommunen skal ha rutiner for å håndtere avvik knyttet til brudd på personopplysningsloven***

Databehandleravtaler

Den tredje problemstillingen er:

- ***Har kommunen oppdaterte «databehandleravtaler»?***

Utledede revisjonskriterier:

- ***Kommunen skal ha databehandleravtaler som fastsetter:***
  - ***varigheten av behandlingen***
  - ***Behandlingens art og formål***
  - ***Typen personopplysninger***
  - ***Kategorier av registrerte***
  - ***Behandlingsansvarliges rettigheter og plikter***
- ***Kommunen må ha avtaler som sikrer at databehandler kun behandler personopplysningene på dokumenterte instrukser fra behandlingsansvarlig***
- ***Kommunen må ha avtaler som setter er klar ramme for hvordan databehandleren kan behandle opplysninger, herunder taushetsplikt***

Nødvendige endringer på IKT-systemer

Den fjerde problemstillingen er:

- ***Har kommunen foretatt nødvendige endringer på IKT?***

Utledede revisjonskriterier:

- ***Kommunen skal iverksette tiltak for å gjøre tilpasninger og rette feil i sine systemer for behandling av personopplysninger som kan medføre risiko for brudd på personvernloven***
- ***Kommunen må ha kartlagt at dens systemer for behandling av personopplysninger bygger på prinsipper om innebygd personvern og personvern som standardinnstilling***

Personvernombud

Den femte problemstillingen er:

- ***Har kommunen et personvernombud med en rolle som er i tråd med regelverket?***

Utledede revisjonskriterier:

- ***Kommunen skal ha et personvernombud***
- ***Behandlingsansvarlig og databehandler skal legge til rette for at personvernombudet får utført sine arbeidsoppgaver i henhold til regelverket***
- ***Personvernombudet skal arbeide uavhengig av behandlingsansvarlig og databehandler og rapportere direkte til det høyeste ledelsesnivået***
- ***Personvernombudet skal informere og gi råd til kommunen om hvilke forpliktelser de har etter regelverket***
- ***Personvernombudet skal kontrollere overholdelsen av regelverket (forordningen)***

4. Personvern i Drammen kommune

4.1. Risiko- og sårbarhetsanalyser (ROS)

Dette kapittelet fokuserer på følgende problemstilling:

- **Har kommunen gjennomført risiko- og sårbarhetsanalyser (ROS)?**

Til denne problemstillingen har vi i kapittel 3 utledet følgende revisjonskriterier:

- **Kommunen skal gi en vurdering av personvernkonsekvenser**
- **Kommunen skal føre protokoller over behandlingsaktiviteter**
- **Kommunen skal gi en vurdering av risikoene for de registrerte rettigheter og friheter**
- **Kommunen skal gi en vurdering av de planlagte tiltakene for å håndtere risikoene, herunder garantier, sikkerhetstiltak og mekanismer for å sikre vern av personopplysningen**

Drammen kommune har en overordnet rutine for arbeid med kartlegging og vurdering av risiko. Det er videre utarbeidet en mal for risiko og sårbarhetsanalyse for personvern. Alle virksomheter skal ta i bruk ROS-analyser «(...) ved innføring av alle typer informasjonssystemer i A4.2 prosjektet[14], ved endringer i, eller innføring av, nye systemløsninger, nye behandlinger, for eksempel overføring til nye parter, endret tilkobling til internett eller andre nettverk»[15].

Vi har også fått oversendt noen eksemplarer av ferdig utfylte ROS-analyser. Vi gjør ikke en analyse av kvaliteten på ROS-analysene, men bemerker seg at mal brukes og medfører at ROS-analyse kan gjennomføres uniformt i hele organisasjonen. Vi bemerker videre at mal for ROS-analyse inneholder de kriteriene som er krevd fra Drammens egen overordnede rutine, samt kravene fra personopplysningsloven.

Personvernkonsekvenser

Når det kommer til vurdering av personvernkonsekvenser, er dette en prosess som alltid skal gjennomføres for alle behandlinger. Artikkel 35 i personvernloven sier at å gjennomføre en vurdering av personvernkonsekvenser (Data Protection Impact Assessment – DPIA), er dette å gjenta denne vurderingen av personvernkonsekvenser, men da med formål om å finne de ekstra tiltakene som trengs for å redusere en høy risiko som man tidligere ikke har klart å redusere. Det vi vurderer her er hvorvidt denne ekstra runden med vurdering av personvernkonsekvenser gjennomføres der hvor risikoen er høy.

[14] A4.2 IKT-prosjektet – prosjektgruppe i kommunesammenslåingsprosessen.
[15] ROS-mal PTL 23.11.2020

Vi er oversendt en gjennomført vurdering av personvernkonsekvenser, samt en mal for når det skal gjennomføres. I mal for gjennomføring av DPIA for Drammen står følgende «Det er obligatorisk å utføre en personvernkonsekvensvurdering (DPIA) dersom det er sannsynlig at en type behandling av personopplysninger kan medføre en høy risiko for fysiske personers personvern, deres rettigheter og friheter (personvernforordningen, artikkel 35)». I den gjennomførte DPIA'en vi er oversendt er det til slutt satt opp 15 risikomomenter, hvorav 6 sies å ha mer en minimal alvorlighetsgrad av risiko. Det er allikevel gjennom DPIA satt inn tiltak som har gjort at alle de 15 risikomomentene har fått en redusert risiko, eller at risikoen er eliminert i sin helhet.

Hvor det er gjort vurderinger om det burde gjennomføres DPIA, og hvor det faktisk er gjennomført en DPIA har fått plass i behandlingsprotokollen som vi har referert til tidligere. Med tanke på at det er et tidlig utkast av behandlingsprotokollen er mest sannsynlig ikke alle lagt inn der, samt at det enkelte steder står at det er anbefalt å gjennomføre DPIA eller at det er påbegynt arbeidet med å gjennomføre DPIA.

Protokoller over behandlingsaktiviteter

Både databehandler, og den behandlingsansvarlige skal ha en protokoll over behandlingsaktiviteter som utføres under deres ansvar. Denne har som funksjon å gi oversikt og sikre bedre kontroll av personvernarbeidet i virksomheten. I Drammen kommune ble arbeidet med utarbeidelse av denne protokollen over behandlingsaktiviteten, heretter omtalt som databehandlerprotkoll, påbegynt høsten 2020. Det siste utkastet som vi ble oversendt var fortsatt mangefult, men vi er informert om at den jobbes kontinuerlig med. Det er Personvernombudet som har tatt fatt på arbeidet.

En fullverdig databehandlerprotokoll skal referere til databehandleravtaler, ROS-analyser, DPIA, behandlingsgrunnlaget og eventuelle andre elementer som virksomheten anser som viktig.

Den registrertes rettigheter

Gjennom personvernloven fremgår det en rekke rettigheter som den registrerte har. Disse rettighetene er rett til; innsyn, retting, sletting, begrensning, å protestere, dataportabilitet, til informasjon, samt enkelte retter når avgjørelser er automatisert. Det er med andre ord viktig at Drammen kommune har oversikt til hvilke rettigheter den enkelte har ved bruk av ulike personopplysninger. Deler av lovverket i personopplysningsloven om den registrertes rettigheter er ikke gjeldene for kommunen. Dette kan sees i sammenheng med sletting, hvor det er personopplysninger kommunen må ha for å kunne gi de tilbudene som det er krav om at den skal gi. Det betyr ikke at kommunen ikke må ha en oversikt, og at vurderinger ikke må gjøres.

Vi har ikke fått en oversikt over hvor det er gjennomført en slik analyse av de registrertes rettigheter, men ser at det er et av punktene som skal besvares når det gjennomføres en DPIA.

Tiltak for å håndtere risiko

Gjennom både de risiko- og sårbarhetsanalysene som er gjennomført, og den DPIA'en vi er oversendt, ser vi at det en av punktene som skal fylles ut handler om å finne tiltak for å håndtere og redusere risikoen. Tiltakene som implementeres er alt fra å utarbeide rutiner til oppdatering av informasjon, det

kan være både konsekvensreduserende tiltak og sannsynlighetsreduserende tiltak. Vi ser blant annet i en ROS-analyse at det refereres til at konsekvensen ved gitt risiko ikke kan reduseres, men man kan minske sannsynligheten for at det inntreffer

Vi har ikke intervjuet eller gjennomført stikkprøver for å se om rutinene er endret, eller om dette er ord uten handling. Etter samtale med personvernombudet er inntrykket vårt at dette blir tatt seriøst av hele virksomheten til Drammen kommune.

Vurdering

Vår vurdering på problemstillingen om kommunen har gjennomført risiko- og sårbarhetsanalyser er at Drammen kommune i dag, når de gjøres, gjennomfører disse i henhold til både egne rutiner og lovkrav. Det må påpekes at det at kommunen ikke har full oversikt over hvor det er, og ikke er gjennomført ROS-analyse.

Ser vi spesifikt på de tre revisjonskriteriene ser vi at det også gjøres vurderinger av personvernkonsekvenser. Vi er dog bare oversendt 1 gjennomført DPIA, og den manglende oppføringen av disse i utkastet til behandlingsprotokollen, gjør det vanskelig å vurdere hvorvidt dette gjøres i alle tilfeller hvor det er behov. Vi ønsker dermed å bemerke at den viktigste anbefalingen vedrørende arbeidet med DPIA er å sikre at alle er registrert i behandlingsprotkollen til Drammen kommune. Dette vil både gi bedre oversikt og øke kontrollmuligheten til personvernombudet og dermed sikre personvernrettighetene til ansatte og innbyggere i Drammen kommune.

Når det kommer til tiltak for å håndtere risiko ser vi at disse både er fremtredende når det gjennomføres ROS-analyser og DPIA. Her er det igjen viktig at oversikten over ROS-analyser og DPIA implementeres i behandlingsprotokollen for å sikre kontroll av arbeidet. Dette kan også gi gevinster ved at der hvor det er mulig kan finnes tiltak som kan implementeres flere steder i virksomheten.

Ut fra vår gjennomgang er vår vurdering at Drammen kommune må sikre at protokollen over behandlingsaktiviteter, eller behandlingsprotokoll som den heter i Drammen kommune, fullføres og oppdateres kontinuerlig. Vi ønsker videre å fremheve at kommunen sikrer at de ulike malene til kommunen vedrørende ROS og DPIA er tilgjengelig og kjent for hele virksomheten.

4.2. Tilpassede rutiner og retningslinjer

Dette kapittelet fokuserer på følgende problemstilling:

- **Har kommunen tilpasset rutiner og retningslinjer?**

Til denne problemstillingen har vi i kapittel 3 utledet følgende revisjonskriterier:

- **Kommunen skal ha et formål med behandling av personopplysninger, og gjennom dette rutiner for å identifisere om det finnes behandlingsgrunnlag**
- **Kommunen skal innhente samtykke der det ikke foreligger annen hjemmel for behandling**
- **Kommunen skal utarbeide personvernerklæring hvor informasjonen er kortfattet, åpen, forståelig og lett tilgjengelig**
- **Kommunen må ha rutiner for sletting av personopplysninger som ikke lengre er nødvendige for formålet de ble samlet inn for**
- **Kommunen skal ha rutiner for å håndtere avvik knyttet til brudd på personopplysningsloven**

Personopplysningsloven tillegger kommunen flerfoldig oppgaver, hvorav det er avgjørende for arbeidet sin del at kommunen har tilpasset rutiner og retningslinjer for å følge opp arbeidet. Revisor har valgt å se nærmere på fire ulike områder for å se om det finnes rutiner og retningslinjer på området, samt hvor utbredt og fungerende disse er.

Formål med behandling (behandlingsgrunnlag)

All behandling av personopplysninger må ha et rettslig grunnlag for å være lov. Et rettslig grunnlag kan være et samtykke eller at man gjennom lovkrav har et rettslig grunnlag. Revisor viser til hvordan dette er gjort i ROS av databehandling for Visma Familie nye Drammen, hvor det vises til at man har lovhjemmel gjennom Barnevernloven §3-1.

Revisor kan ikke se at kommunen har spesifikke rutiner for å identifisere om det finnes behandlingsgrunnlag i seg selv. Vi har heller ikke fått oversendt dokumentasjon som tilsvarer at det er gjennomført noe opplæring i regi av kommunen. Vi er informert om at det er sendt ut en brosjyre for omtrent to år siden på tematikken.

I de tidligere nevnte risiko- og sårbarhetsanalysene som systemforvaltere i kommunen skal gjennomføre er en av punktene som må besvares om det finnes behandlingsgrunnlag. Dette kan anses som en rutine for å identifisere om det finnes behandlingsgrunnlag.

Samtykke

Der hvor det ikke er hjemmel i lov som gir behandlingsgrunnlag må kommunen be om samtykke for å innhente og bruke personopplysningene til sine ansatte og innbyggere. Som vi nevnte ovenfor ser vi at det ved gjennomføring av ROS-analyser skal det identifiseres om det finnes behandlingsgrunnlag, og det er der hvor lovkrav ikke automatisk gir behandlingsgrunnlag at man må ta i bruk samtykke.

Den tidligere nevnte behandlingsprotokollen skal til slutt å oversikt over hvert enkelt samtykkebasert behandlingsgrunnlag.

Vi er oversendt enkelte samtykkeskjemaer fra Drammen kommune

- **Skjema for Samtykke bilder og film, ansatte Drammen kommune**
- **Skjema for Tilbaketrekking av samtykke**
- **Gjennomføring av opptak av lyd, bilde og film hos tjenestemottaker**
- **Veileder for opptak av lyd, bilde og film i helse- og omsorgstjenester**
- **Samtykkeskjema - ny pasient**

Ut ifra disse samtykkeskjemaene anslår vi at det ikke finnes noen felles mal for hvordan disse skal utarbeides.

Personvernerklæring

Drammen kommune har lagt ut en personvernerklæring på sine nettsider. Under lenken personvern[16] har kommunen beskrevet hovedtrekkene i forhold til hva de betyr for deg, hvordan du skal gå frem. Her fremkommer det hvilken adgang kommunen har til å samle personopplysninger, hvordan kommunen behandler personopplysninger og eventuelt hvilke klagemuligheter du har. Områdene som er beskrevet, er:

- **Vern av personopplysninger**
- **Personvernombud**
- **Offentlighet, innsyn og postlister**
    - **Publisering av saksdokumenter på Internett**
    - **Innsynsrett i offentlige dokumenter**
- **Logging og statistikk**
- **Tredjepart**

I sin omtale har kommunen lenket videre til relevante nettsider hos Datatilsynet.

Omtalen av tredjepart tar for seg forholdet til det som kalles informasjonskapsler («cookies»). Detter betyr at enkelte opplysninger om brukerens bruk av nettsider (som drammen.kommune.no) lagres på brukerens datamaskin i små tekstfiler, som skal gi brukere tilgang til ulike funksjoner på nettstedet. Dette er en vanlig metode for å logge hvilke sider brukerne besøker, og opplysningene benyttes for å forbedre brukeropplevelsen og videreutvikle nettstedet.

Det er ingen omtale av det som omhandler en eventuell tredjeparts behandling av personopplysninger. Det man ofte vil tenke på som tredjepart i forhold til når andre behandler data på vegne av kommunen.

[16] Personopplysninger og personvern | Drammen kommune

I tillegg har kommunen lagt ut informasjon om personvern i barnehagen[17] og personvern i skolen[18]. Her omtales hva personvern er, hvilke regler som gjelder og det lenkes videre til Datatilsynets informasjon om regler rundt filming, bilder, presse (media), kontaktlister/klasselister, samt loggføring av elevers internettbruk.

Ut over dette er vi ikke forelagt noe generell personvernerklæring.

Sletting

Sletting av personopplysninger er en viktig del av personopplysningsloven. Kravet er så sterkt at det er forbudt å oppbevare personopplysninger lengre enn det som er nødvendig for formålet de ble samlet inn for. Vi ønsker å presisere at dette betyr at det i slike situasjoner skal slettes uten at de som er registrert har bedt om det. Mye av den kommunale virksomheten er på bakgrunn av andre lovkrav unntatt kravet om sletting. Det vil allikevel være viktig å ha rutiner for å sikre at en slik vurdering gjøres, samt at der hvor kravet om sletting står, skal det være rutiner for å sikre at dette gjennomføres.

I de tidligere nevnte ROS'ene som skal gjennomføres er en av punktene i malen til Drammen kommune at det skal gjøres vurdering av hvor lenge personopplysningene skal behandles/lagres. I de to ferdig utfylte ROS'ene vi er tilsendt er det i begge tilfeller henvist til arkivloven som årsak til at det ikke skal automatisk slettes. Vi har dermed ikke sett noen vurdering hvor det må slettes, og dermed ikke sett hvordan man da hadde gått frem for å slette.

Gjennom samtale med personvernombudet kom det frem at sletting reguleres i databehandleravtalene, og at data vil slettes når avtalene løper ut. Dette er ikke nødvendigvis et godt nok tiltak, da lengden på en databehandleravtale kan være lengre enn tidsrammen som retten på sletting av personopplysninger.

Avvik

Et avvik er et brudd på personopplysningssikkerheten. Ved et avvik skal det rapporteres innen 72 timer etter at avviket er oppdaget til Datatilsynet. Man er unntatt forpliktelsen om å melde til datatilsynet om bruddet sannsynligvis ikke vil medføre en risiko for fysiske personers rettigheter og friheter. Ved avvik må det dermed tidlig gjøres en vurdering over sannsynligheten for at det vil medføre en risiko for fysiske personers rettigheter og friheter.

Vi er oversendt et dokument om intern avvikshåndtering hvor det fremkommer hvilke vurderinger man skal gjøre ved et avvik, hvem som har ansvaret og hvem man skal rapportere til.

Vurdering

Drammen kommune har mye rutiner og retningslinjer i arbeidet med personvern i egen virksomhet. Kommunen har rutiner for å vurdere behandlingsgrunnlaget gjennom de ROS-analysene som

[17] Personvern i barnehagen | Drammen kommune
[18] Personvern i skolen | Drammen kommune

gjennomføres, Gjennom de samme ROS-analysene vil det fremkomme hvorvidt det trengs samtykke. Kommunen har per dags dato ikke totaloversikt over alle stedene hvor det brukes samtykke, noe som er viktig for å få oversikt over hvilke personopplysninger kommunen samler inn. Det vil også ofte i situasjoner hvor det kreves samtykke, også være strengere krav knyttet til sletting av personopplysninger.

Vi er ikke informert om at kommunen har noen rutiner for å sikre at personopplysninger som ikke lenger er nødvendige, og som ikke kan lagres hjemlet i andre lovkrav, slettes. Her er det viktig at Drammen kommune opparbeider seg oversikt, og får på plass systemer og rutiner som sikrer at personopplysninger som skal slettes, faktisk slettes.

4.3. Databehandleravtaler

Dette kapittelet fokuserer på følgende problemstilling:

- Har kommunen oppdaterte «databehandleravtaler»?

Til denne problemstillingen har vi i kapittel 3 utledet følgende revisjonskriterier:

- Kommunen skal ha databehandleravtaler som fastsetter:
  - varigheten av behandlingen
  - Behandlingens art og formål
  - Typen personopplysninger
  - Kategorier av registrerte
  - Behandlingsansvarliges rettigheter og plikter
- Kommunen må ha avtaler som sikrer at databehandler kun behandler personopplysningene på dokumenterte instrukser fra behandlingsansvarlig
- Kommunen må ha avtaler som setter er klar ramme for hvordan databehandleren kan behandle opplysninger, herunder taushetsplikt

En databehandleravtale er en avtale mellom databehandler og behandlingsansvarlig om hvordan personopplysninger skal behandles. Det er et krav om å ha en slik databehandleravtale der hvor man benytter seg av en underleverandør. Drammen har ikke en totaloversikt over alle sine databehandlere per dags dato, det er identifisert omtrent 60 databehandleravtaler, og den tidligere nevnte databehandlerprotokollen skal i fremtiden ha oversikt over alle databehandleravtalene.

Vi er oversendt en rekke ulike databehandleravtaler, vi velger å ikke vurdere kvaliteten på avtalene, men har sett gjennom dem for å se om de opprettholder de kravene som vi har valgt å se etter gjennom revisjonskriteriene. Vi er også oversendt et dokument som viser til at man skal bruke DFØ[19]

[19] DFØ = Direktoratet for forvaltning og økonomistyring

sin mal for databehandleravtaler, men er informert om at dette ikke alltid er mulig. Dette kan være fordi aktørene er for store og ønsker å bruke egne maler, eller fordi det tidligere ikke har vært tydelige nok retningslinjer og rutiner om at man skal bruke DFØ sin mal.

Vi er informert om at det er et pågående arbeid med å sikre at databehandleravtalene så ofte som mulig skal bruke DFØ sin mal, eller i det minste oversettes til norsk om det er andre aktører sin mal som skal brukes. Vi er videre informert om personvernombudet har hatt et økt søkelys på databehandleravtaler, hvor det blant annet er ryddet opp i gamle avtaler og oppdatert disse. En årsak til slik oppdatering kan være at man har brukt en mal uten å fylle ut all informasjonen som skal fylles ut, noe vi også har sett i enkelte av de databehandleravtalene vi er tilsendt.

Et eksempel på dette ser vi i databehandleravtaler med TurnitIN hvor standardteksten for åpne felt ikke er fylt inn:

> *«Turnitin LLC, 2101 Webster Street, Suite 1800, Oakland CA 94612 USA (the "Processor"); and [Institution name and address] (the "Controller");»*

Vi er også informert om at det er en noe manglende kompetanse både i Drammens egen virksomhet, men også ute blant leverandørene om når det er behov for en databehandleravtale og hvorvidt man er selvstendig behandlingsansvarlig eller en databehandler.

Vurdering

Det at malene brukes uten at all informasjon oppdateres til å nevne virksomhet gjør det vanskeligere å vurdere hvorvidt det er gjort egne vurderinger i avtalen. Det at man dermed kan være tvilende på om informasjonen om hvilke personopplysninger databehandleravtalen gjelder er riktig, er et kritisk moment som er viktig at løses opp i. Vi er informert om at dette er noe som arbeides med av personvernombudet, og at dette er noe som har fokus. Vi ønsker allikevel å påpeke viktigheten av at denne informasjonen oppdateres.

Vi vil anbefale at i de tilfeller hvor det fravikes fra å bruke DFØ sin mal for databehandleravtale, bør det vedlegges et dokument som gir en forklaring hvorfor dette valget er gjort. Det kan finnes gode grunner for å avvike, men da er det viktig at denne vurderingen tydeliggjøres.

Vi ønsker også å trekke frem at den manglende kompetansen i egen virksomhet er viktig å ta tak i. Personvernlovgivningen er komplisert, og det at det hersker tvil om når en databehandleravtale skal tas i bruk viser til at det er behov for å sikre at kompetansen heves, samt at alle kjenner til personvernombudet og dens funksjon.

4.4. Nødvendige endringer på IKT-systemer

Dette kapittelet fokuserer på følgende problemstilling:

- **Har kommunen foretatt nødvendige endringer på IKT?**

Til denne problemstillingen har vi i kapittel 3 utledet følgende revisjonskriterier:

- **Kommunen skal iverksette tiltak for å gjøre tilpasninger og rette feil i sine systemer for behandling av personopplysninger som kan medføre risiko for brudd på personvernloven**
- **Kommunen må ha kartlagt at dens systemer for behandling av personopplysninger bygger på prinsipper om innebygd personvern og personvern som standardinnstilling**

Virksomhet IKT har utarbeidet en IKT strategi hvor det legges opp til bruk av tre rammeverk, TOGAF[20], ITIL[21] og ISO 27001[22]. De opplyser at det varierer hvor langt kommunen har kommet med implementeringen av disse. Ansatte som skal arbeide med rammeverkene har gått på kurs og noen har fullført sertifisering.

Ved etableringen av den nye kommunen ble det etablert et prosjekt for å migrere og slå sammen systemer for bruk i nye Drammen kommune. Det ble gjennomført en ROS-analyse av databehandlingen i alle systemer i porteføljen. Fra mal for ROS-analyse fremgår det at systemet skal kategoriseres og plasseres i en av tre kategorier.

- **Ingen personopplysninger**
- **Personopplysninger**
- **Personopplysninger av særlig kategori.**

For de systemene som behandlet personopplysninger ble det stilt tilleggsspørsmål som systemeier måtte besvare.

Det opplyses videre at alle systemer som ble migrert inn i nye Drammen kommune hadde vært gjennom en Deployment Advisory Board (DAB). Dette er en formell overlevering fra prosjekt til Drift. Men at det med det store antall systemer og mengden av systemer som skulle migreres innen oppstart av ny kommune, naturligvis ble identifisert risiko som ikke ble behandlet med tiltak i forkant av overlevering. Prosjekt A4.2 – IKT prosjektet, har brukt 2020 til å følge opp tiltak.

[20] TOGAF (The Open Group Architecture Framework) er et åpent rammeverk for arkitektur.
[21] ITIL (Information Technology Infrastructure Library) er en strukturert livssyklus rammeverk for leveranser av IKT-tjenester
[22] ISO/IEC 27001 Standard som gir retningslinjer for etablering, implementering, drift, vedlikehold, evaluering og forbedring av en organisasjons ledelsessystem for informasjonssikkerhet.

I kommunens mal for vurdering av personvernkonsekvenser (DPIA) fremgår det at man vurderer om de forskjellige områdene i personvernlovgivningen er godt nok beskrevet i forhold til hvordan systemet håndterer disse, det vurderes risiko, og det settes opp tiltak som må/bør vurderes.

Personvernombudet har i påvente av at kommunen får på plass en protokoll over behandlingsaktiviteter, startet å bygge opp en oversikt (behandlingsprotokoll) på eget initiativ. I denne fremgår det ikke om det er vurdert om systemene trenger å endres, hvilke behov for endring som eventuelt er avdekket, når endringer er planlagt eller om endringene er bestilt/gjennomført.

Vurdering

I den dokumentasjon vi er forelagt kan vi ikke se at kommunen har en strukturert oversikt over hvilket behov de har for å gjøre tilpasninger / endringer på sine IKT-systemer for å tilfredsstille personvernlovgivningen. Eller hvilken status det er på dette arbeidet.

I kommunens mal for ROS-analyse er det generelle betraktninger om hvorvidt det er en risiko rundt behandling av personvernopplysninger. I kommunens mal for DPIA fremgår det mer detaljerte vurderinger rundt behandling av personvernopplysninger. Men vi har i liten grad sett at dette er benyttet, kommunen har ingen god sentral oversikt over hvilke systemer dette er gjennomført for, og hvilken status det er på eventuelle tiltak disse vurderingene har medført.

Vår vurdering er at kommunen trenger å prioritere arbeidet med å sikre at kartlegginger er eller blir gjennomført, og lage sentrale oversikter/systemer for oppfølging av de tiltak som disse medfører.

4.5. Personvernombud

Dette kapittelet fokuserer på følgende problemstilling:

- Har kommunen et personvernombud med en rolle som er i tråd med regelverket?

Til denne problemstillingen har vi i kapittel 3 utledet følgende revisjonskriterier:

- Kommunen skal ha et personvernombud
- Behandlingsansvarlig og databehandler skal legge til rette for at personvernombudet får utført sine arbeidsoppgaver i henhold til regelverket
- Personvernombudet skal arbeide uavhengig av behandlingsansvarlig og databehandler og rapportere direkte til det høyeste ledelsesnivået
- Personvernombudet skal informere og gi råd til kommunen om hvilke forpliktelser de har etter regelverket
- Personvernombudet skal kontrollere overholdelsen av regelverket

Etablering av et personvernombud

Drammen kommune har hatt personvernombud siden 2018. Det første personvernombud sluttet etter en tid i stillingen sin, og frem til nytt personvernombud ble ansatt i februar 2020 var det formelle ansvaret lagt til en jurist hos kommuneadvokaten. Det er viktig å påpeke at det nye personvernombudet tiltrådte sin stilling rett i forkant av utbruddet av Covid-19, og de restriksjonene som har kommet i tiden etter dette har påvirket oppstarten av arbeidet.

Arbeidsoppgaver, uavhengighet og rapportering

Grunnmuren for arbeidsoppgavene til personvernombudet er definert ut fra det personvernforordningen artikkel 39 sier om stillingen. Gjennom samtale med personvernombudet fremkom det at rollen til ikke er klart definert utenfor dette. Oppgavene til personvernombudet er stort sett tilknyttet Risiko- og sårbarhetsanalyser, databehandleravtaler og vurdering av personvernkonsekvenser. Mye av dette arbeidet kommer gjennom at det tas kontakt med personvernombudet med spørsmål om de tre områdene.

Personvernombudet arbeider med planlegging av fremtidig arbeid, men på grunn av flere etterspørsler fra virksomheter rundt ROS, DPIA og DBA, har dette vært vanskelig å gjennomføre. Det er også igangsatt et arbeid med behandlingsprotokollen for hele virksomheten som personvernombudet har tatt ansvar for.

Personvernombudet rapporterer til nivå 2 i Drammen kommunens styringssystem, til leder for fellestjenester. Kommunens organisering er bygd opp slik at i nivå 1 finner man kommunedirektøren (Rådmann) og direktørene for styring og eierskap, samfunn samt utvikling og digitalisering. Planen er en årlig gjennomgang og rapporter11ing, men det er uttalt av personvernombudet at det er ønskelig med mellom 1 til 4 gjennomganger med ledelsen i året. Personvernombudet har også fått en indirekte linje til toppledelsen med opprettelsen av, og deltagelse i det nyopprettede informasjonssikkerhetsrådet.

Personvernombudets rolle som informerende, rådgivende og kontrollerende

Som nevnt tidligere er en av de med tidkrevende oppgavene til personvernombudet å svare på e-poster med virksomheter som ønsker tilbakemeldinger på utarbeidelse av ROS-analyser og databehandleravtaler. Når nytt personvernombud ble ansatt i februar var en av ønskene om at det skulle være virksomhetsbesøk for å gjøre hele virksomheten kjent med det nye personvernombudet, men også øke bevisstheten omkring hva et personvernombud kan bistå med. Dette arbeidet ble utsatt på bakgrunn av den pågående pandemien, men vi er informert om at ønske om å gjennomføre det fortsatt er der.

Som vi har nevnt tidligere går store deler av arbeidsdagen til personvernombudet i dag til å svare på e-poster i en rådgivende funksjon.

Vurdering

Drammen kommune har et personvernombud med en rolle som er i tråd med regelverket. Det kan allikevel påpekes at personvernombudet sitter med arbeidsoppgaver som er utenfor det regelverket

spesifiserer, og som kan resultere i en rollekonflikt. Vi ønsker å presisere at dette ikke nødvendigvis er feil, men er noe blant annet Datatilsynet også advarer om i sine veiledere på nettsidene sine. Personvernombudet sitter i dag med enkelte utførende arbeidsoppgaver da det ikke er noen andre som gjør dem, og ikke fordi de er pålagt.

Den ene anbefalingen rundt personvernombudet omhandler ikke personvernombudet i seg selv, men at de i dag utførende arbeidsoppgavene som personvernombudet gjør da den ser at det ikke gjennomføres om ikke, må kommunen ta tak i og gjennomføre. Det kan tyde på at det i dag ikke er nok ressurser i personvernarbeidet til Drammen kommune sin virksomhet, og for å ta igjen det tapte er det viktig at det settes inn mer ressurser og at fokuset på alle nivåer i organisasjonen økes..

Vi ønsker også å anbefale om at det sikres at personvernombudet rapporterer direkte til øverste nivå, altså nivå 1 i Drammen sitt styringsnivå. Personvernloven dikterer at personvernombudet skal rapportere direkte til høyeste ledelsesnivå, og da slik vi ser det må personvernombudet i Drammen kommune rapportere direkte til nivå 1, som består av kommunedirektøren (Rådmann) og direktørene for styring og eierskap, samfunn samt utvikling og digitalisering.

5. Oppsummering og konklusjon

Drammen kommune har i dag en positiv utvikling i sitt arbeid med personvern. Rutiner, retningslinjer og maler utarbeides og bidrar til et mer uniformt arbeid med personvern i hele virksomheten til kommunen. Dette ble veldig tydelig når vi så gjennom risiko- og sårbarhetsanalysene rundt personvern, samt når det ble gjennomført vurdering av personvernkonsekvenser (Data Protection Impact Assessment – DPIA).

Det samme så vi ved databehandleravtalene, hvor det tidligere var mangler i hvilke databehandleravtaler man brukte, samt utfyllingen av disse. Her har fokuset gått over til å bruke DFØ sin mal, samt oppdatere og rette tidligere databehandleravtaler hvor det var mangler.

Det fellestrekket vi har sett gjennom å gå gjennom Drammen kommune sitt personvernarbeid, er at det i dag eksisterer mangler som stammer fra tidligere og at det vil kreve ressurser for å sikre at dette arbeidet kommer à jour. I dag ser mye av dette arbeidet til å være lagt på personvernombudet sine skuldre, ikke fordi det pålegges, men fordi personvernombudet ser at ikke andre tar tak i det. Dette sees blant annet med behandlingsprotokollen, en lovpålagt protokoll som Drammen kommune enda ikke har en fullverdig versjon av.

Den mottatte dokumentasjonen gir inntrykk av at kommunen ikke har noen strukturert oversikt over behovet for å gjøre tilpasninger / endringer på IKT-systemer for å tilfredsstille personvernlovgivningen, eller hvilken status det er på dette arbeidet. Kommunen har etter vår vurdering gode maler for analyser og vurderinger på personvernområdet, men vi kan ikke se at disse er gjennomført for store deler av området eller at det er ført noen oversikt over status med dette arbeidet. Vi mener derfor at kommunen må prioritere arbeidet med å sikre at kartlegginger er eller blir gjennomført, samt utarbeide en oversikt over oppfølging av de tiltak som disse medfører.

Endringene som fulgte av kommunesammenslåingen hvor tre kommuner ble en, samt en IKT-virksomhet som lå «på siden» av kommunen og nå er en del av kommunens basisorganisasjon virker å ha gitt mange utfordringer på IKT-området. Dette gjelder blant annet alt arbeidet som er lagt ned i forbindelse med valg av systemer, endringer og tilpasninger, justering av brukeradferd, ROS-analyser, informasjonssikkerhet og personvern. I denne «kampen» om fokus og prioritering virker det på oss som om personvern og personvernombudet ikke har nådd så høyt opp på prioriteringslisten som hadde vært ønskelig.

6. Anbefaling

Med bakgrunn i vår gjennomgang vil vi anbefale kommunedirektøren / Drammen kommune å gjennomføre følgende:

- **Sørge for tilstrekkelige ressurser for å sikre at protokoller over behandlingsaktiviteter fullføres.**
- **Sikre at det utarbeides en sentral oversikt (system) for å holde oversikt over kartlegging av behov for nødvendige endringer på IKT og status på tiltak som disse medfører**
- **Sikre at kompetansen og forståelsen om personvernlovgivningen er tilstrekkelig i egen virksomhet.**
- **Vurdere å endre rapporteringsnivået for personvernombudet fra nivå 2 til nivå 1.**

Et utkast til rapport har blitt oversendt kommunedirektøren til uttalelse. Kommunedirektørens uttalelse i brev av 19. februar 2021 er vedlagt rapporten.

Drammen, den 23. februar 2021.

Torkild Halvorsen
Leder forvaltningsrevisjon

Frode H Christoffersen
Oppdragsansvarlig forvaltningsrevisor

Jonas Strisland
Forvaltningsrevisor

Referanser

LOV 2018-06-22 nr 83 – Lov om kommuner og fylkeskommuner (kommuneloven)
I kraft fra og med det konstituerende møtet i det enkelte kommunestyret og fylkestinget ved oppstart av valgperioden 2019-2023

LOV 1992-09-25 nr 107 – Lov om kommuner og fylkeskommuner (kommuneloven)

LOV 2018-12-20 nr 116, Lov om behandling av personopplysninger (personopplysningsloven)

FOR 2018-06-15 nr 876, Forskrift om behandling av personopplysninger

EUROPAPARLAMENTS- OG RÅDSFORORDNING (EU) 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt om oppheving av direktiv 95/46/EF (generell personvernforordning)

Prop. 56 LS (2017–2018), Lov om behandling av personopplysninger (personopplysningsloven) og samtykke til deltakelse i en beslutning i EØS-komiteen om innlemmelse av forordning (EU) nr. 2016/679 (generell personvernforordning) i EØS-avtalen

Datatilsynet:

- Datatilsynet - personvern og informasjonssikkerhet | Datatilsynet
  - **Personvernprinsippene:** Personvernprinsippene | Datatilsynet
  - **Dine rettigheter:** Dine rettigheter | Datatilsynet
  - **Virksomhetenes plikter:** Virksomhetenes plikter | Datatilsynet
  - **Personvernombud:** Personvernombud | Datatilsynet
    - Hvordan sikre ombudets uavhengighet? | Datatilsynet
  - **Vurdering av personvernkonsekvenser og forhåndsdrøftelse:** Vurdering av personvernkonsekvenser og forhåndsdrøftelse | Datatilsynet
  - **Protokoll over behandlingsaktiviteter / Den behandlingsansvarliges protokoll / Databehandlerens protokoll:** Protokoll over behandlingsaktiviteter | Datatilsynet
  - **Innebygget personvern:** Innbygd personvern | Datatilsynet
  - **Ordliste – personvern:** Ordliste | Datatilsynet
- **Datatilsynets personvernerklæring:** Datatilsynets personvernerklæring | Datatilsynet

Dokumenter fra Drammen kommune som er forelagt revisjonen i dette prosjektet:

- **Internkontroll – Informasjonssikkerhet – Overordnet ROS-vurdering – Sentral IT-løsning, D-IKT**
- **Virksomhet IKT – Oppsummering BIA samtaler (Business Impact Analysis)**
- **Et utvalg ROS-analyser for IKT-systemer**
- **Et utvalg databehandleravtaler for IKT-systemer**
- **Etiske regler**
- **Samfunnssikkerhet og beredskap**
- **Organisasjonskart**
- **Overordnede prinsipper for ledelse, styring og kontroll**
- **Overordnet retningslinje for digital sikkerhet**

- Rådmannens delegeringsreglement
- Organisering av informasjonssikkerhet
- Rollebeskrivelse forvaltning av IKT-systemer
- IKT – Strategi – Nye Drammen – 2018 - 2022
- Sourcingstrategi
- Arkitekturstrategi for nye Drammen
- Tekniske IT-krav for nye løsninger
- Porteføljestyring i Drammen kommune
- Kartlegging og vurdering av risiko
- Mal for Risiko- og sårbarhetsanalyse av databehandlingen – Personvern, tekniske- og organisatoriske forhold, A4.2 IKT prosjektet
- Mal for gjennomføring av DPIA (Data Protection Impact Assessment) / Personvernkonsekvensvurdering
- Mal for databehandleravtale
    - lenket videre til Databehandleravtale og sjekkliste | Anskaffelser.no
- Rutine for avviksmelding til Datatilsynet
- Melding og behandling av hendelser
- Prosedyre for offentlighet og innsyn i postlister
- Skjema for Samtykke bilder og film, ansatte Drammen kommune
- Gjennomføring av opptak av lyd, bilde og film hos tjenestemottaker
- Veileder for opptak av lyd, bilde og film i helse- og omsorgstjenester
- Samtykkeskjema - ny pasient
- Skjema for Tilbaketrekking av samtykke
- Taushetserklæring
- Politiattest
- Rekrutteringsprosessen - huskeliste
- Konflikter og krevende personalsaker - rutine for håndtering
- Kriterier velferdsteknologi
- Retningslinje-Fjerntilgang (hjemmekontor)
- Sjekkliste – kvalitetssikring i Public 360 for desentrale arkivtjenester
- Sjekkliste for systematisk forbedringsarbeid

I tillegg er vi forelagt følgende dokumenter som er under utarbeidelse:

- Behandlingsprotokoll – under utarbeidelse
- Rutine for personvern ved anskaffelse av nye informasjonssystemer
- Rutine for henvendelse for innsyn/retting/sletting av personopplysninger
- Hvem har rett til informasjon om barnet? (Vigilo – barnehager og skoler)
- Intern avvikshåndtering

www.drammen.kommune.no

- Personvernerklæring:
    - Personopplysninger og personvern | Drammen kommune
    - Personvernombud | Drammen kommune
    - Opplysninger til tredjepart | Drammen kommune
    - Personvern i skolen | Drammen kommune
    - Personvern i barnehagen | Drammen kommune

Vedlegg 1 – Uttalelse fra kommunedirektøren, datert 19. februar 2021

DRAMMEN KOMMUNE

VIKEN KOMMUNEREVISJON IKS
Postboks 4197
3005 DRAMMEN

Dato: 19.02.2021
Saksnr.: 21/09235-2
Deres ref.:

~~Unntatt offentlighet Offl. § 5~~

Rådmannens uttalelse til utkast rapport - Personvern

Rådmannen har mottatt utkast til rapport etter Vikens kommunerevisjons forvaltningsrevisjon innen personvern, til uttalelse.
Arbeidet med personvern har vært prioritert i forkant av kommunesammenslåingen. Eksempelvis ble det opprettet felles personvernombud for Svelvik, Drammen og Nedre Eiker og et nært samarbeid rundt personvern og informasjonssikkerhet. I tiden etter sammenslåingen har det vært viktig å fortsette dette arbeidet.
Fremover ser rådmannen et behov for at det arbeides videre med å skape gode strukturer. De forslag som fremkommer i forvaltningsrevisjonens rapport, ser rådmannen som viktige innspill i det videre arbeidet.
Ut over dette har rådmannen følgende kommentarer til de konkrete anbefalinger i rapporten
Anbefaling: *Sørge for tilstrekkelige ressurser for å sikre at protokoller over behandlingsaktiviteter fullføres.*
Arbeidet med behandlingsprotokoll er pågående. Rådmannen vurderer at svakhetene som påpekes vil avhjelpes når behandlingsprotokollen er fullstendig. Kommunen har anskaffet et systemverktøy, Ardoq, som på sikt skal sørge for at vi til enhver tid har oversikt over behandlingsaktiviteter, integrasjon og infrastruktur.
Vurdering av kapasitet på området sees i sammenheng med det årlige arbeidet med økonomiplan.

Anbefaling: *Sikre at det utarbeides en sentral oversikt (system) for å holde oversikt over kartlegging av behov for nødvendige endringer på IKT og status på tiltak som disse medfører.*
I arbeidet med å etablere ny kommune ble det gjort et grundig arbeid med personvernhensyn i kommunens IKT systemer. Dette er et kontinuerlig arbeid og rådmannen vil prioritere arbeidet fremover. Dammen kommune har nylig besluttet en ny digitaliseringsstrategi og personvern er viktig en del av denne strategien.

Anbefaling: *Sikre at kompetansen og forståelsen om personvernlovgivningen er tilstrekkelig i egen virksomhet.*

Ved ansettelse av nytt personvernombud, fikk kommunen styrket sin kompetanse på fagområdet. Personvernombudet har fått tildelt oppgaver som skal påse at kommunen får utnyttet kompetansen i størst mulig grad. Kommunen er i en fase hvor det prioriteres å få utarbeidet gode systemer, rutiner og å sørge for kompetanseheving hos ansatte. Personvernombudet har hatt og har en viktig rolle for

Styring og eierskap

Fellestjenester
Organisasjonsnummer

Postadresse
Postboks 7500
3008 DRAMMEN

Besøksadresse
Engene 1
3015 DRAMMEN

Telefon

koordinering og opplæring. Personvernombudet sitter også i kommunens informasjonssikkehetsråd som koordinerer tiltak innenfor personvern og informasjonssikkerhet.

Anbefaling: *Vurdere å endre rapporteringsnivået for personvernombudet fra nivå 2 til nivå 1.*

Ved utformingen av organisasjonsstrukturen i ny kommune, ble det foretatt en vurdering av hva som ville være en hensiktsmessig plassering av personvernombudet. Det ble vurdert at organiseringen og rapporteringsstrukturen som ble valgt, ivaretok lovkravet. Når det gjelder organisatorisk plassering i organisasjonen, anså rådmannen det mest sentralt at personvernombudet kunne ivareta sin uavhengige rolle og sin faglige integritet.
Etter forvaltningsrevisjonens rapport, vil rådmannen likevel gjøre en ny vurdering.

Med hilsen

Erik Brun-Pedersen
Stabsleder Fellestjenester

Dokumentet er sendt elektronisk uten underskrift

Kopi: Pål Tore Larsen

Vedlegg 2 – RSK 001 – Standard for forvaltningsrevisjon

Nedenfor følger et kort resyme av RSK 001, med de viktigste punktene som skal følges.

> ***Fastsatt av NKRFs styre 12.08.2020 og gjort gjeldende som god kommunal revisjonsskikk for forvaltningsrevisjoner med oppstartsbrev sendt etter 30.09.2020.***

Standarden er bygget opp med 34 punkter bestående av grunnleggende prinsipper og revisjonshandlinger i forvaltningsrevisjon, hvor noen er anbefalinger og noen er obligatoriske krav. Standarden fastsetter normer for planlegging, gjennomføring og rapportering av forvaltningsrevisjon i kommuner, fylkeskommuner og i (fylkes)kommunalt eide selskap.

Gjennomføring av forvaltningsrevisjon er en lovpålagt oppgave i kommuner og fylkeskommuner[23], og kontrollutvalget skal påse at det utføres forvaltningsrevisjon. Det skal utarbeides en plan for forvaltningsrevisjon som viser på hvilke områder det skal gjennomføres forvaltningsrevisjoner. Denne skal baseres på en risiko- og vesentlighetsvurdering, og den skal vedtas av kommunestyret eller fylkestinget selv.

Forvaltningsrevisjon innebærer å gjennomføre systematiske vurderinger av økonomi, produktivitet, regeletterlevelse, måloppnåelse og virkninger ut fra kommunestyrets eller fylkestingets vedtak og forutsetninger. Forvaltningsrevisjon skal ikke overprøve politiske prioriteringer som er foretatt av kommunens eller fylkeskommunens folkevalgte organer.

Punkt	Innhold
	Innledning
1-3	Krav til revisor
4-8	Bestilling og problemstilling
9-13	Revisjonsdialogen
14-15	Revisjonskriterier
16-19	Metode og data
20-22	Vurderinger og konklusjoner
23	Anbefalinger
24-28	Rapport
29-31	Dokumentasjon
32-34	Kvalitetssikring og kvalitetskontroll

Krav til revisor:

Det skal utpekes en oppdragsansvarlig for hvert oppdrag i forvaltningsrevisjon, og denne er ansvarlig for å påse at standardens krav er oppfylt. Oppdragsansvarlig revisor skal sikre at forvaltningsrevisjonen gjennomføres med tilstrekkelig kunnskap om og ferdigheter i relevante metoder, og med tilstrekkelig kunnskap om temaet som revisjonen omhandler. Revisor skal være uavhengig og objektiv ved utførelsen av sine oppgaver.

Bestilling og problemstilling:

Forvaltningsrevisjonen skal gjennomføres i samsvar med kontrollutvalgets bestilling, og revisor skal vurdere om kontrollutvalgets bestilling lar seg gjennomføre. Revisor skal forsikre seg om at kontrollutvalget og revisor har lik forståelse av oppdraget, at rammene er tilstrekkelig klarlagt, og om nødvendig avklare bestillingen med kontrollutvalget.

Revisor skal sikre at det utarbeides problemstillinger som er tilstrekkelig konkretisert og avgrenset til å kunne besvares, og at de er egnet til å besvare kontrollutvalgets bestilling. Dersom det er behov for å endre problemstillinger underveis slik at det kan ha betydning for gjennomføringen av oppdraget, skal dette avklares med kontrollutvalget.

Revisor skal utarbeides en skriftlig prosjektplan for hver forvaltningsrevisjon, som redegjør for problemstillinger, revisjonskriterier eller grunnlaget for disse, og metodebruk.

Revisjonsdialogen:

Revisor skal iverksette tiltak som er egnet til å sikre god dialog med revidert enhet, øvrige involverte og andre relevante aktører. Senest før datainnsamling starter skal revisor sende oppstartsbrev til kommunedirektøren (alt.

[23] LOV 2018-06-22 nr 83, Lov om kommuner og fylkeskommuner (kommuneloven), syvende del, kapittel 22 til 26, §§ 22-1 til 26-1

selskapet). Som hovedregel skal det avholdes oppstartsmøte hvor det redegjøres for bakgrunn, problemstillinger, revisjonskriterier, informasjonsbehov og planlagt gjennomføring av forvaltningsrevisjonen.

Utkast til rapport skal sendes kommunedirektøren (alt. selskapet som er gjenstand for forvaltningsrevisjon), og uttalelsen skal fremgå av rapporten i sin helhet. Endelig rapport skal oversendes kontrollutvalget, med kopi til kommunedirektøren (alt. selskapet).

Revisjonskriterier:

Med utgangspunkt i problemstillinger skal revisor etablerere revisjonskriterier utledet fra autoritative eller anerkjente kilder innenfor det reviderte området. Kildene skal presenteres for revidert enhet, som skal gis anledning til å komme med innspill. Revisjonskriteriene skal være relevante, konkrete og i samsvar med de kravene som gjelder for revidert enhet innenfor den aktuelle tidsperioden.

Metode og data:

Revisor skal sikre dataenes relevans (gyldighet, validitet) for problemstillingen, og datainnsamlingen skal gjennomføres på en måte som sikrer dataenes pålitelighet (reliabilitet). Metodevalg skal begrunnes og eventuelle svakheter i datamaterialet skal synliggjøres. Det skal innhentes data i tilstrekkelig omfang til å kunne gjøre vurderinger og svare på problemstillingene. Data som er fremkommet muntlig skal nedtegnes skriftlig og bekreftes av kilden. Personopplysninger skal behandles i tråd med kravene i personopplysningsloven.

Vurderinger, konklusjoner og anbefalinger:

Revisor skal vurdere innsamlede data opp mot revisjonskriteriene, og dersom det avdekkes vesentlige avvik skal det komme tydelig frem i rapporten. Vurderinger må være objektive, og med bakgrunn i disse skal revisor konkludere i forhold til problemstillingene.

Anbefalinger er ikke obligatorisk, men skal gis der dette er hensiktsmessig ut fra data, vurderinger og konklusjoner. Anbefalinger skal ikke gis i form av detaljerte løsninger.

Rapport:

Det skal skrives rapport til hvert forvaltningsrevisjonsprosjekt, og rapporten skal utformes så leservennlig som mulig med hensyn til språk og struktur.

Rapporten skal vise sammenhengen ("den røde tråden") mellom problemstillinger, revisjonskriterier, innsamlede data, vurderinger, konklusjoner og eventuelle anbefalinger, og det skal være et klart skille mellom hva som er presentasjon av data (fakta) og hva som er revisors vurderinger. Praksis eller tilstand innen det reviderte området skal beskrives i et omfang som i tilstrekkelig grad underbygger revisors vurderinger og konklusjoner.

Dokumentasjon:

Forvaltningsrevisjon skal dokumenteres på en måte som er tilstrekkelig til å gi en totalforståelse av utførelsen av prosjektet, og til å underbygge revisors vurderinger og konklusjoner. Forhold som tilsier at det kan foreligge misligheter eller feil, skal dokumenteres særskilt. Det samme gjelder dersom det avdekkes åpenbare brudd på annet regelverk enn det som inngår i revisjonen. Dokumentasjon skal oppbevares i minst 10 år.

Kvalitetssikring og system for kvalitetskontroll

Utførelse av forvaltningsrevisjon skal kvalitetssikres, og denne skal dokumenteres. Den skal sikre at undersøkelse og rapport har nødvendig faglig og metodisk kvalitet og følger denne standard.

Revisjonsenheten skal dokumentere et system for kvalitetskontroll.

Vedlegg 3 – Metode

Prinsipper for metodebruk i forvaltningsrevisjon følger av *"RSK 001 Standard for forvaltningsrevisjon"*[24] som er vedtatt av Norges Kommunerevisorforbund (NKRF). Denne bygger i stor grad på samfunnsvitenskapelig metode om etterprøvbarhet av funn, og rettslige prinsipper om at revidert enhet skal kunne få frem sitt syn (kontradiksjon) ut fra vår gjennomgang og vurdering av område vi ser på.

Sett i lys av en forvaltningsrevisjons begrensede ressursramme, samt hensiktsmessigheten i forhold til dens formål, er dokumentasjonen og sikring av denne ikke så omfattende som kravene som settes til vitenskapen og domstolene. Ut fra en vitenskapelig og filosofisk side er det ingen informasjon/dokumentasjon som er helt objektiv eller kilde som er 100% pålitelig.

I forvaltningsrevisjon tilstreber vi at vurderinger og anbefalinger skal gjøres på et objektivt og etterprøvbart grunnlag. Ofte er problemstillingene i en forvaltningsrevisjon mer lukkede og definerte enn forskning og etterforskning. Dette påvirker også våre valg av metode. En av hovedhensiktene med forvaltningsrevisjon er å få til læring og endring om det vurderes behov for dette. Ofte vil dette også skje gjennom prosessen når vi gjennomfører en forvaltningsrevisjon. Ved at det settes fokus på et tema og/eller område, vil ofte den reviderte selv se behov for endring.

Det å pålegge endring er en politisk prosess som er gjenstand for saksbehandling. Av den grunn vil ikke våre vurderinger få direkte virkning for å sette i gang endringsprosesser. Gjennom å fremme vurderinger, og eventuelt anbefalinger, som er relevante for problemstillingene søker vi å bidra til utvikling i den reviderte enhet.

I prosjekter kan vi benytte oss av kvalitative og kvantitative metoder[25]. Kvalitativ metode vektlegger forståelse og analyse av sammenhenger i en prosess hos den enkelte. De er viktige for å utvikle bedre forståelse av individer, i forhold til for eksempel motivasjon, følelser, holdninger og kognitive prosesser. Kvantitativ metode består av opptelling av fenomener eller kjennetegn ved en gruppe individer. Det brukes for å analysere et stort antall enheter, som for eksempel land, personer eller bedrifter. Kvalitative og kvantitative metoder er supplerende metoder som ikke kan erstatte hverandre.

Eksempler på aktuelle metoder for innsamling og analyse av informasjon / fakta ved forvaltningsrevisjon:

- **Dokumentanalyse**
- **Samtaler / intervju / gruppeintervju**
- **Spørreundersøkelser**
- **Statistiske analyser**
- **Trendanalyser**

---

[24] Vedlegg 2 – RSK 001 – Standard for forvaltningsrevisjon
[25] Store norske leksikon – https://snl.no/kvalitativ_metode og https://snl.no/kvantitativ_metode

- Økonomiske analyser (som regnskapsanalyse)
- Case
- Scenarioanalyse
- Observasjon

I denne revisjonen har vi benyttet følgende metoder:

Dokumentanalyse

Dokumentanalyse består av å hente informasjon fra planer, rapporter, rutiner, vedtak, referater og lignende.

Styrkene ved dokumentanalyse er at informasjonen er skriftlig, og i mange tilfeller har flere personer vært involvert i utarbeidelsen av den. Er dokumentasjonen utarbeidet av den reviderte kan den antas å ha stor grad av pålitelighet. Er dokumentasjonen utarbeidet av, eller på vegne av, noen med en saksinteresse, er det grunn til å være mer forsiktig i bruken av dem.

Dokumentanalyse er ofte hensiktsmessig i forvaltningsrevisjon, siden det ofte finnes mange dokumenter med relevante data for våre undersøkelser. Svakheten er at dokumentanalyse i seg selv bare fanger opp det som er skriftlig dokumentert. For å motvirke dette vil dokumentanalyse ofte benyttes i kombinasjon med andre metoder.

Samtaler / intervju / gruppeintervju

Samtaler, intervju og/eller gruppeintervju egner seg godt til å undersøke åpne, beskrivende problemstillinger, og særlig der det er begrenset med skriftlig informasjon / dokumentasjon.

Utfordringer er å vurdere om det i tilstrekkelig grad gir et helhetlig og «korrekt» bilde av virkeligheten. Utvalgets størrelse og hvordan man velger ut hvem som skal intervjues vil ha betydning for påliteligheten.

Ved gjennomføring av intervjuer skal det føres referat fra samtalen, og de som er intervjuet skal i ettertid verifisere at referatet gir en riktig fremstilling av deres syn på et tema og/eller område.

Vedlegg 4 – Utledning av revisjonskriterier

Undersøkelsen har 5 problemstillinger:

- **Har kommunen gjennomført risiko- og sårbarhetsanalyser (ROS)?**
- **Har kommunen tilpasset rutiner og retningslinjer?**
- **Har kommunen oppdaterte «databehandleravtaler»?**
- **Har kommunen foretatt nødvendige endringer på IKT?**
- **Har kommunen et personvernombud med en rolle som er i tråd med regelverket?**

For hver av disse har revisjonen utledet revisjonskriterier. Kriteriene er ikke nødvendigvis uttømmende for ethvert krav som stilles til alle sider av arbeidet innenfor personvern i Drammen kommune. Kriteriene er oppstilt etter revisjonens vurdering av hva som er det sentrale, basert på en vurdering av virksomhetens egenart og regelverket den forvalter.

Problemstillingene og de utledede revisjonskriteriene er omtalt samlet i kapittel 3.

Risiko- og sårbarhetsanalyser (ROS)

- ***Har kommunen gjennomført risiko- og sårbarhetsanalyser (ROS)?***

Utledede revisjonskriterier:

- ***Kommunen skal gi en vurdering av personvernkonsekvenser (artikkel 35, 1)***
- ***Kommunen skal føre protokoller over behandlingsaktiviteter (artikkel 30)***
- ***Kommunen skal gi en vurdering av risikoene for de registrerte rettigheter og friheter (artikkel 35, 7c)***
- ***Kommunen skal gi en vurdering av de planlagte tiltakene for å håndtere risikoene, herunder garantier, sikkerhetstiltak og mekanismer for å sikre vern av personopplysningen (artikkel 35, 7d)***

Kilder og begrunnelse:

Det er sagt i personopplysningsloven artikkel 35, 1 at den behandlingsansvarlige skal foreta en vurdering før behandlingen av hvilke konsekvenser den planlagte behandlingen vil ha for personopplysningsvernet. Vurderingen skal gjøres dersom det er sannsynlig at en type behandling, særlig bruk av ny teknologi og idet tas hensyn til behandlingens art, omfang, formål og sammenhengen den utføres i, vil medføre en høy risiko for fysiske personers rettigheter. En vurdering kan omfatte flere lignende behandlingsaktiviteter som innebærer høye risikoer.

Personopplysningslovens artikkel 35 7c og d fremhever at behandlingsansvarlig skal gjøre en vurdering av risikoene for de registrertes rettigheter og friheter, slik det er nevnt i artikkelens første avsnitt. Vurderingen skal inneholde de planlagte aktivitetene for å håndtere risikoene, hvilket er de garantier, sikkerhetstiltak og mekanismer for å sikre vern av personopplysninger og for å påvise at

forordningen overholdes, når det tas hensyn til de registrertes og andre personers rettigheter og berettigede interesser.

Personopplysningslovens artikkel 30 pålegger den behandlingsansvarlige å føre protokoll over behandlingsaktiviteter. Protokoll skal blant annet inneholde informasjon om navnet på og kontaktopplysningene til den behandlingsansvarlige (og hvis relevant, den felles behandlingsansvarlige, den behandlingsansvarliges representant og personvernombudet), formålene med behandlingen, en beskrivelse av kategoriene av registrerte og kategoriene av personopplysninger, kategoriene av mottakere som personopplysningene er blitt eller vil bli utlevert til, overføringer av personopplysninger til en tredjestat eller en internasjonal organisasjon hvis dette er relevant, de planlagte tidsfristene for sletting av de forskjellige kategoriene av opplysninger hvis det er mulig og en generell beskrivelse av de tekniske og organisatoriske sikkerhetstiltakene nevnt i artikkel 32 nr. 1 dersom det er mulig.

Databehandler skal føre en protokoll over alle kategorier av behandlingsaktiviteter som er utført på vegne av en behandlingsansvarlig. Denne skal blant annet inneholde navnet på og kontaktopplysningene til databehandleren eller databehandlerne og til hver behandlingsansvarlig som databehandleren opptrer på vegne av (og hvis relevant, den behandlingsansvarliges eller databehandlerens representant og personvernombudet), kategoriene av behandling utført på vegne av hver behandlingsansvarlig, overføringer av personopplysninger til en tredjestat eller en internasjonal organisasjon dersom det er relevant og en generell beskrivelse av de tekniske og organisatoriske sikkerhetstiltakene nevnt i artikkel 32 nr. 1 dersom det er mulig.

Protokollene skal være skriftlige (herunder elektroniske) og skal på anmodning gjøre protokollen tilgjengelig for tilsynsmyndigheten.

Tilpassede rutiner og retningslinjer

- *Har kommunen tilpasset rutiner og retningslinjer?*

Utledede revisjonskriterier:

- *Kommunen skal ha et formål med behandling av personopplysninger (artikkel 6a), og gjennom dette rutiner for å identifisere om det finnes behandlingsgrunnlag (artikkel 6)*
- *Kommunen skal innhente samtykke der det ikke foreligger annen hjemmel for behandling (artikkel 7 (1))*
- *Kommunen skal utarbeide personvernerklæring hvor informasjonen er kortfattet, åpen, forståelig og lett tilgjengelig (artikkel 12 (1))*
- *Kommunen må ha rutiner for sletting av personopplysninger som ikke lengre er nødvendige for formålet de ble samlet inn for (artikkel 17a)*
- *Kommunen skal ha rutiner for å håndtere avvik knyttet til brudd på personopplysningsloven (artikkel 33/34).*

Kilder og begrunnelse:

Personopplysningslovens artikkel 6 redegjør for behandlingen av personopplysningers lovlighet og sier at behandlingen bare er lovlig dersom minst ett av artikkelens vilkår er oppfylt. Blant annet skal den registrerte samtykke til behandling av sine personopplysninger for ett eller flere spesifikke formål. Videre er det åpnet for behandling av personopplysninger dersom det er nødvendig; for å oppfylle en avtale som den registrerte er part i, for å oppfylle en rettslig forpliktelse som påhviler den behandlingsansvarlige, for å verne den registrertes eller en annen fysisk persons vitale interesser, for å utføre en oppgave i allmennhetens interesse eller utøve offentlig myndighet som den behandlingsansvarlige er pålagt eller 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. Det siste gjelder særlig dersom den registrerte er et barn.

Artikkel 7 sier at dersom behandlingen av personopplysningene bygger på samtykke, skal den behandlingsansvarlige kunne påvise at den registrerte har samtykket til behandling av personopplysninger. Dersom den registrertes samtykke gis i forbindelse med en skriftlig erklæring som også gjelder andre forhold, skal anmodningen om samtykke fremlegges på en måte som gjør at den tydelig kan skilles fra nevnte andre forhold, i en forståelig og lett tilgjengelig form og på et klart og enkelt språk. Den registrerte har til enhver tid rett til å trekke tilbake sitt samtykke.

Artikkel 12 presiserer at klar og tydelig informasjon og kommunikasjon er viktig. Den behandlingsansvarlige skal treffe egnede tiltak for å fremlegge for den registrerte informasjon ved innsamling av personopplysninger, ønske om innsyn og retting og sletting av opplysninger, samt all kommunikasjon knyttet til dette på en kortfattet, åpen, forståelig og lett tilgjengelig måte.

I artikkel 17 fremkommer det at den registrerte skal ha rett til å få personopplysninger om seg selv slettet av den behandlingsansvarlige dersom personopplysningene ikke lenger er nødvendige for formålet som de ble samlet inn eller behandlet for. Dette gjelder også dersom det ikke ligger grunn til videre behandling, eller at personopplysningene ikke er blitt behandlet lovlig.

Personopplysningslovens artikkel 33 sier at dersom det oppstår et brudd på personopplysningsloven skal den behandlingsansvarlige uten grunnet opphold og når det er mulig, og senest 72 timer etter å ha fått kjennskap til bruddet, skal bruddet meldes til tilsynsmyndighet. Dersom behandlingsansvarlig ikke får meldt ifra innen 72 timer, skal årsakene til forsinkelsen redegjøres for. Artikkel 33 tredje ledd redegjør for at meldingen skal beskrive hva bruddet gjelder, når det er mulig, kategoriene av og omtrent antall registrerte som er berørt, samt hvilke personopplysninger som er berørt. Behandlingsansvarlig skal beskrive de sannsynlige konsekvensene av personopplysningssikkerheten, samt hvilke tiltak som behandlingsansvarlig har truffet eller foreslår å treffe for å håndtere bruddet på personopplysningssikkerheten. Sannsynlige konsekvenser av brudd på personopplysningssikkerheten skal beskrives.

Artikkel 34 første ledd sier at dersom det er sannsynlig at bruddet på personopplysningssikkerheten vil medføre en høy risiko for fysiske personers rettigheter og friheter, skal den behandlingsansvarlige uten ugrunnet opphold underrette den registrerte om bruddet. Underrettingen til de det gjelder skal gi en klar og tydelig beskrivelse av arten av bruddet på personopplysningssikkerheten.

Databehandleravtaler

- ***Har kommunen oppdaterte «databehandleravtaler»?***

Utledede revisjonskriterier:

- ***Kommunen skal ha databehandleravtaler som fastsetter:***
  - ***varigheten av behandlingen***
  - ***Behandlingens art og formål***
  - ***Typen personopplysninger***
  - ***Kategorier av registrerte***
  - ***Behandlingsansvarliges rettigheter og plikter (artikkel 28 1)***
- ***Kommunen må ha avtaler som sikrer at databehandler kun behandler personopplysningene på dokumenterte instrukser fra behandlingsansvarlig (artikkel 28 3a)***
- ***Kommunen må ha avtaler som setter er klar ramme for hvordan databehandleren kan behandle opplysninger, herunder taushetsplikt (datatilsynet/artikkel 28 3b)***

Kilder og begrunnelse:

Det er sagt i Personopplysningslovens artikkel 28 første ledd at dersom en behandling skal utføres på vegne av en behandlingsansvarlig, skal den behandlingsansvarlige benytte seg av databehandlere som gir tilstrekkelige garantier for at de vil gjennomføre egnede tekniske og organisatoriske tiltak som. sikrer at behandlingen oppfyller kravene gitt i forordningen og vern av de registrertes rettigheter. Artikkel 28 tredje ledd sier at behandling utført av en databehandler skal være underlagt en avtale eller annet rettslig dokument som er bindende for databehandleren med hensyn til den behandlingsansvarlige, varigheten av behandlingen, behandlingens art og formål, typen personopplysninger og kategorier av registrerte, samt den behandlingsansvarliges rettigheter og plikter.

I avtalen skal det angis at databehandleren behandler personopplysningene etter gitte dokumenterte instrukser fra den behandlingsansvarlige. Databehandleren kan ikke overføre personopplysninger til en tredjestat eller en internasjonal organisasjon, med mindre det kreves av EU-retten eller nasjonal rett som databehandleren er underlagt. I så fall må behandlingsansvarlig bli underrettet om dette, med mindre rett av hensyn til viktige allmenne interesser forbyr en slik underretning. I avtalen skal det også fremkomme at databehandleren skal sikre at personer som er autorisert til å behandle personopplysninger, har forpliktet seg til å behandle opplysningene konfidensielt eller er underlagt en egnet lovfestet taushetsplikt.

Nødvendige endringer på IKT-systemer

- ***Har kommunen foretatt nødvendige endringer på IKT?***

Utledede revisjonskriterier:

- ***Kommunen skal iverksette tiltak for å gjøre tilpasninger og rette feil i sine systemer for behandling av personopplysninger som kan medføre risiko for brudd på personvernloven. (kommuneloven § 25-1 og personvernloven artikkel 24, 25 og 26)***
- ***Kommunen må ha kartlagt at dens systemer for behandling av personopplysninger bygger på prinsipper om innebygd personvern og personvern som standardinnstilling (artikkel 25)***

Kilder og begrunnelse:

Av kommunelovens § 25-1 følger det at kommunen skal ha internkontroll med administrasjonens virksomhet for å sikre at lover og forskrifter følges. Det er kommunedirektøren som er ansvarlig for internkontrollen. Internkontrollen skal være systematisk og tilpasses virksomhetens størrelse, egenart, aktiviteter og risikoforhold, og ved internkontroll skal kommunedirektøren:

a) utarbeide en beskrivelse av virksomhetens hovedoppgaver, mål og organisering
b) ha nødvendige rutiner og prosedyrer
c) avdekke og følge opp avvik og risiko for avvik
d) dokumentere internkontrollen i den formen og det omfanget som er nødvendig
e) evaluere og ved behov forbedre skriftlige prosedyrer og andre tiltak for internkontroll.

Personopplysningslovens artikkel 24 pålegger den behandlingsansvarlige å gjennomføre egnede tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen utføres i samsvar med denne forordning. Tiltakene skal gjennomgås på nytt og oppdateres ved behov. Dette skal ta hensyn til behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter,

I artikkel 25 fremgår det at systemer som behandler personopplysninger skal utformes etter prinsippene om innebygd personvern og personvern som standardinnstilling. Av første ledd fremgår det at den behandlingsansvarlige skal gjennomføre egnede tekniske og organisatoriske tiltak som er utformet med sikte på en effektiv gjennomføring av prinsippene for vern av personopplysninger, og for å integrere de nødvendige garantier i behandlingen for å oppfylle kravene i denne forordning og verne de registrertes rettigheter.

Av andre ledd fremgår det at den behandlingsansvarlige skal gjennomføre egnede tekniske og organisatoriske tiltak for å sikre at det som standard bare er personopplysninger som er nødvendige for hvert spesifikke formål med behandlingen, som behandles. Dette får følger for den mengden personopplysninger som samles inn, omfanget av behandlingen av opplysningene, hvor lenge de lagres og deres tilgjengelighet. Disse tiltakene skal særlig sikre at personopplysninger som standard ikke gjøres tilgjengelige for et ubegrenset antall fysiske personer uten den berørte personens medvirkning.

Personopplysningslovens artikkel 28 pålegger den behandlingsansvarlige å bruke en databehandler som gir tilstrekkelige garantier for at de vil gjennomføre egnede tekniske og organisatoriske tiltak som sikrer at behandlingen oppfyller kravene i denne forordning og vern av den registrertes rettigheter.

Personvernombud

- ***Har kommunen et personvernombud med en rolle som er i tråd med regelverket?***

Utledede revisjonskriterier:

- ***Kommunen skal ha et personvernombud (artikkel 37 (1,3,6)***
- ***Behandlingsansvarlig og databehandler skal legge til rette for at personvernombudet får utført sine arbeidsoppgaver i henhold til regelverket (artikkel 38 (2).***
- ***Personvernombudet skal arbeide uavhengig av behandlingsansvarlig og databehandler og rapportere direkte til det høyeste ledelsesnivået (artikkel 38 (3))***
- ***Personvernombudet skal informere og gi råd til kommunen om hvilke forpliktelser de har etter regelverket (forordningen) (artikkel 39 1a)***
- ***Personvernombudet skal kontrollere overholdelsen av regelverket (forordningen) (artikkel 39 1b)***

Kilder og begrunnelse:

Personopplysningsloven artikkel 37 sier at den behandlingsansvarlige og databehandleren skal utpeke et personvernombud når:

- **behandlingen utføres av en offentlig myndighet eller et offentlig organ,**
- **når den behandlingsansvarlige eller databehandlerens kjernevirksomhet består av behandlingsaktiviteter som på grunn av sin art, omfang og/eller formål krever regelmessig og systematisk overvåkning i stor skala av registrerte.**
- **Den behandlingsansvarliges eller databehandlerens kjernevirksomhet består av behandling i stor skala av særlige kategorier av opplysninger i henhold til artikkel 9 eller personopplysninger om straffedommer og lovovertredelser.**

***Offentlige myndigheter eller offentlige organ kan utpeke ett personvernombud for flere av nevnte myndigheter eller organer, med hensyn til deres organisasjonsstruktur og størrelse. Personvernombudet kan være ansatt hos den behandlingsansvarlige eller hos databehandleren eller utføre oppgavene på grunnlag av en tjenesteavtale. Personvernombudet skal utpekes på grunnlag av faglige kvalifikasjoner og på særlig grunnlag av dybdekunnskap om personvernlovgivning og praksis på området samt evne til utføre oppgavene knyttet til informasjon og rådgivning, kontrollere overholdelse av regelverk og samarbeid med tilsynsmyndighetene.**

Av artikkel 38 fremgår det at behandlingsansvarlig og databehandleren skal støtte personvernombudet i forbindelse med utførelsen av oppgavene knyttet til informasjon og rådgivning,

kontrollere overholdelse av regelverk og samarbeid med tilsynsmyndighetene ved å stille nødvendige ressurser til rådighet. De skal gi tilgang til personopplysninger og behandlingsaktiviteter og gjøre det mulig for vedkommende å opprettholde sin dybdekunnskap. Behandlingsansvarlig og databehandler skal sikre at personvernombudet ikke tar imot instrukser om utførelsen av nevnte oppgaver. Personvernombudet skal ikke avsettes eller straffes av den behandlingsansvarlige eller databehandleren for å utføre sine lovpålagte oppgaver. Personvernombudet skal rapportere direkte til det høyeste ledelsesnivået hos den behandlingsansvarlige eller databehandleren.

Artikkel 39 redegjør for personvernombudets oppgaver. Personvernombudet skal informere og gi råd til den behandlingsansvarlige eller databehandleren og de ansatte som utfører behandlingen, om de forpliktelsene de har i henhold til forordningen og andre bestemmelser om vern av personopplysninger. Personvernombudet skal kontrollere overholdelsen av forordningen og den behandlingsansvarliges eller databehandlerens personvernretningslinjer, herunder fordeling av ansvar, holdningsskapende tiltak og opplæring av personellet som er i involvert i behandlingsaktivitetene, og tilhørende revisjoner.

Vedlegg 5 – Definisjoner

Hentet fra *«EUROPAPARLAMENTS- OG RÅDSFORORDNING (EU) 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt om oppheving av direktiv 95/46/EF (generell personvernforordning)»*

Artikkel 4. Definisjoner

I denne forordning menes med

1) «personopplysninger» **enhver opplysning om en identifisert eller identifiserbar fysisk person («den registrerte»); en identifiserbar fysisk person er en person som direkte eller indirekte kan identifiseres, særlig ved hjelp av en identifikator, f.eks. et navn, et identifikasjonsnummer, lokaliseringsopplysninger, en nettidentifikator eller ett eller flere elementer som er spesifikke for nevnte fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sosiale identitet,**

2) «behandling» **enhver operasjon eller rekke av operasjoner som gjøres med personopplysninger, enten automatisert eller ikke, f.eks. innsamling, registrering, organisering, strukturering, lagring, tilpasning eller endring, gjenfinning, konsultering, bruk, utlevering ved overføring, spredning eller alle andre former for tilgjengeliggjøring, sammenstilling eller samkjøring, begrensning, sletting eller tilintetgjøring,**

3) «begrensning av behandling» **merking av lagrede personopplysninger med det som mål å begrense behandlingen av disse i framtiden,**

4) «profilering» **enhver form for automatisert behandling av personopplysninger som innebærer å bruke personopplysninger for å vurdere visse personlige aspekter knyttet til en fysisk person, særlig for å analysere eller forutsi aspekter som gjelder nevnte fysiske persons arbeidsprestasjoner, økonomiske situasjon, helse, personlige preferanser, interesser, pålitelighet, atferd, plassering eller bevegelser,**

5) «pseudonymisering» **behandling av personopplysninger på en slik måte at personopplysningene ikke lenger kan knyttes til en bestemt registrert uten bruk av tilleggsopplysninger, forutsatt at nevnte tilleggsopplysninger lagres atskilt og omfattes av tekniske og organisatoriske tiltak som sikrer at personopplysningene ikke kan knyttes til en identifisert eller identifiserbar fysisk person,**

6) «register» **enhver strukturert samling av personopplysninger som er tilgjengelig etter særlige kriterier, enten samlingen er plassert sentralt, er desentralisert eller spredt på et funksjonelt eller geografisk grunnlag,**

7) «behandlingsansvarlig» **en fysisk eller juridisk person, en offentlig myndighet, en institusjon eller ethvert annet organ som alene eller sammen med andre bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes; når formålet med og midlene for behandlingen er fastsatt i unionsretten eller i medlemsstatenes nasjonale rett, kan den behandlingsansvarlige, eller de særlige kriteriene for utpeking av vedkommende, fastsettes i unionsretten eller i medlemsstatenes nasjonale rett,**

8) «databehandler» **en fysisk eller juridisk person, offentlig myndighet, institusjon eller ethvert annet organ som behandler personopplysninger på vegne av den behandlingsansvarlige,**

9) «mottaker» **en fysisk eller juridisk person, offentlig myndighet, institusjon eller ethvert annet organ som personopplysninger utleveres til, enten det dreier seg om en tredjepart eller ikke. Offentlige myndigheter som kan motta personopplysninger innenfor rammen av en særskilt undersøkelse i samsvar med unionsretten eller medlemsstatenes nasjonale rett, skal imidlertid ikke anses som mottakere; nevnte offentlige myndigheters behandling av slike opplysninger skal være i samsvar med gjeldende regler om vern av personopplysninger i henhold til formålet med behandlingen,**

10) «tredjepart» **enhver annen fysisk eller juridisk person, offentlig myndighet, institusjon eller ethvert annet organ enn den registrerte, den behandlingsansvarlige, databehandleren og de personer som under den behandlingsansvarlige eller databehandlerens direkte myndighet har fullmakt til å behandle personopplysninger,**

11) «samtykke» **fra den registrerte 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,**

12) «brudd på personopplysningssikkerheten» **et brudd på sikkerheten som fører til utilsiktet eller ulovlig tilintetgjøring, tap, endring, ulovlig spredning av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet,**

13) «genetiske opplysninger» **personopplysninger om en fysisk persons nedarvede eller ervervede genetiske egenskaper som gir unik informasjon om den aktuelle fysiske personens fysiologi eller helse, og som særlig er framkommet etter analysering av en biologisk prøve fra den aktuelle fysiske personen,**

14) «biometriske opplysninger» **personopplysninger som stammer fra en særskilt teknisk behandling knyttet til en fysisk persons fysiske, fysiologiske eller atferdsmessige egenskaper, og som muliggjør eller bekrefter en entydig identifikasjon av nevnte fysiske person, f.eks. ansiktsbilder eller fingeravtrykksopplysninger,**

15) «helseopplysninger» **personopplysninger om en fysisk persons fysiske eller psykiske helse, herunder om ytelse av helsetjenester, som gir informasjon om vedkommendes helsetilstand,**

16) «hovedvirksomhet»:

a) når det gjelder en behandlingsansvarlig med virksomheter i mer enn én medlemsstat, stedet for dennes hovedadministrasjon i Unionen, med mindre avgjørelser om formål og midler i forbindelse med behandlingen av personopplysninger treffes i en annen av den behandlingsansvarliges virksomheter i Unionen, og sistnevnte virksomhet har myndighet til å få gjennomført nevnte avgjørelser, i dette tilfellet skal virksomheten som har truffet slike avgjørelser, anses for å være hovedvirksomheten,

b) når det gjelder en databehandler med virksomheter i mer enn én medlemsstat, stedet for dennes hovedadministrasjon i Unionen eller, dersom databehandleren ikke har noen hovedadministrasjon i Unionen, databehandlerens virksomhet i Unionen der hoveddelen av behandlingsaktivitetene i forbindelse med aktivitetene ved en databehandlers virksomhet finner sted, i den grad databehandleren er underlagt særlige forpliktelser i henhold til denne forordning,

17) «representant» **en fysisk eller juridisk person som er etablert i Unionen, som den behandlingsansvarlige eller databehandleren har utpekt skriftlig i henhold til artikkel 27, og som representerer den behandlingsansvarlige eller databehandleren med hensyn til de forpliktelser de har i henhold til denne forordning,**

18) «foretak» **en fysisk eller juridisk person som utøver økonomisk virksomhet, uavhengig av foretakets rettslige form, herunder partnerskap eller sammenslutninger som regelmessig utøver økonomisk virksomhet,**

19) «konsern» **et foretak som utøver kontroll, og dets kontrollerte foretak,**

20) «bindende virksomhetsregler» **retningslinjer for vern av personopplysninger som en behandlingsansvarlig eller databehandler som er etablert på en medlemsstats territorium, følger i forbindelse med en overføring eller en rekke overføringer av personopplysninger til en behandlingsansvarlig eller databehandler i én eller flere tredjestater internt i et konsern eller gruppe av foretak som utøver en felles økonomisk virksomhet,**

21) «tilsynsmyndighet» **en uavhengig offentlig myndighet som er opprettet av en medlemsstat i henhold til artikkel 51,**

22) «berørt tilsynsmyndighet» **en tilsynsmyndighet som er berørt av en behandling av personopplysninger, fordi**

a) **den behandlingsansvarlige eller databehandleren er etablert på territoriet til nevnte tilsynsmyndighets medlemsstat,**

b) **registrerte som er bosatt i nevnte tilsynsmyndighets medlemsstat, i vesentlig grad påvirkes eller sannsynligvis vil bli påvirket av behandlingen, eller**

c) **det er klaget til nevnte tilsynsmyndighet,**

23) «grenseoverskridende behandling»

a) **behandling av personopplysninger som finner sted i forbindelse med aktiviteter i en behandlingsansvarligs eller databehandlers virksomheter i mer enn én medlemsstat, dersom den behandlingsansvarlige eller databehandleren er etablert i mer enn én medlemsstat, eller**

b) **behandling av personopplysninger som finner sted i forbindelse med aktiviteter i en behandlingsansvarligs eller databehandlers eneste virksomhet i Unionen, men som i betydelig grad påvirker eller sannsynligvis vil påvirke registrerte i mer enn én medlemsstat.**

24) «relevant og begrunnet innsigelse» **en innsigelse mot et utkast til avgjørelse om hvorvidt det foreligger en overtredelse av denne forordning eller om hvorvidt et planlagt tiltak som gjelder den behandlingsansvarlige eller databehandleren, er i samsvar med denne forordning, og som tydelig viser betydningen av risikoene som utkastet til avgjørelse utgjør med hensyn til de registrertes grunnleggende rettigheter og friheter og, dersom det er relevant, den frie flyten av personopplysninger i Unionen,**

25) «informasjonssamfunnstjeneste» **en tjeneste som definert i artikkel 1 nr. 1 bokstav b) i europaparlaments- og rådsdirektiv (EU) 2015/1535,**

26) «internasjonal organisasjon» **en organisasjon og dens underordnede organer som er underlagt folkeretten, eller ethvert annet organ opprettet ved eller på grunnlag av en avtale mellom to eller flere stater.**

Vi kan kommuner

Viken kommunerevisjon IKS
Org.nr.: 985 731 098 MVA
post@vkrevisjon.no | vkrevisjon.no

Hovedkontor - Drammen
Postadresse: Postboks 4197, 3005 Drammen
Besøksadresse: Øvre Eiker vei 14, 3048 Drammen

Avdelingskontor - Hønefoss
Postadresse: Postboks 123, Sentrum, 3502 Hønefoss
Besøksadresse: Osloveien 1, 3511 Hønefoss

Avdelingskontor - Follo
Postadresse: Postboks 173, 1401 Ski
Besøksadresse: Parkaksen 7, 1400 Ski

Avdelingskontor - Hallingdal
Besøksadresse: Alfarvegen 177, 3540 Nesbyen