Årsrapport 2021

Personvernombudet

i

Oslo kommune

Innhold

1. Innledning

For et utrent øye har ikke Oslo kommune noen store problemer når det gjelder arbeidet med personvern (og informasjonssikkerhet). Oversikter for 2021 viser liten grunn til bekymring og indikerer grundig arbeid og godt lederskap:

- Rapporteringen om ledelsens gjennomgang (LG) og virksomhetens egenerklæring (VE) er gjennomført som planlagt i stort sett alle virksomheter
- En økning i antall avvik som er meldt til Datatilsynet vekker tillit: Vi tar personvern på alvor og prioriterer kvalitetsarbeid og prosessforbedring
- Kommunen fikk ikke nevneverdig kritikk fra Datatilsynet i 2021; kun ett gebyr ble gitt (i forbindelse med en eldre sak om fulltekstpublisering av sensitive personopplysninger) og ingen særskilte saker ble fulgt opp fra tilsynets side (bortsett fra noen nylig tilsendte tilleggsspørsmål knyttet til en tidligere sak om personvernet i fagsystemet Gerica)
- Kommunens sentrale fagmiljø for personvern og informasjonssikkerhet merker stor pågang og mange spørsmål og ulike arrangementer som faste fagforum har stor deltakelse og gode tilbakemeldinger

Det er likevel ingen grunn til å lene seg tilbake og tenke at «- Dette ordnet vi fint». Personvern er på ingen måte tilstrekkelig innarbeidet i Oslo kommunes mangslungne virksomhet. Arbeidet må pågå kontinuerlig og det trengs styrket innsats på en rekke områder.

Denne årsrapporten viser at historien gjentar seg: Som tidligere år vil ombudet legge stor vekt på avvikshåndtering og ressursallokering; med andre ord ledelse…

2. Anbefalinger

- Alle ledere bør ha en gjennomgang av avviksrutinene i sin virksomhet. Om lag halvparten av kommunens virksomheter meldte ingen avvik til Datatilsynet i 2021. Mørketallene i Oslo kommune er åpenbart store. En positiv utvikling her forutsetter en bevisstgjøring og kulturbygging som må komme fra ledere – på alle nivåer.
- Byrådsavdelingene må prioritere arbeidet med personvern og informasjonssikkerhet. Med unntak av BLK, OVK og FIN/ISI har personvernombudet vært minimalt i kontakt med byrådsavdelingene.
- Et minimum av kompetansehevende tiltak bør gjøres obligatorisk for alle kommunens ansatte (ikke minst ledere).
- Kommunen bør prioritere arbeidet med en strategi for digital transformasjon og IKT. Denne strategien bør se på blant annet
    - Reorganisering av digitaliseringsarbeidet i kommunen som helhet, med fokus på tydeligere rolle- og ansvarsfordeling for alle impliserte virksomheter
    - Revisjon av Oslo kommunes IKT-reglement og alle tilhørende instrukser
- Oslo kommune har arbeidet for å få på plass et styringssystem for informasjonssikkerhet (SSIS/ISMS). I tillegg til dette bør kommunen arbeide for å få på plass et styringssystem for personvern (SSPV/PIMS).
- Alle virksomheter bør gjennomføre en personvernvurdering av bruken av kommunikasjonskanaler som for eksempel sosiale medier som minimum en vurdering på overordnet nivå, men helst en full personvernkonsekvensvurdering (DPIA).
- Alle virksomheter må passe på at de har en oppdatert behandlingsoversikt.
- Virksomhetene må se til at personvernkoordinatorene har nok tid og kompetanse til å gjøre oppgavene sine. Bydelene må i særdeleshet få styrket sin ressurstilgang.
- Personvernombudet eller andre fagressurser bør bli bedt om å gi informasjon/opplæring til kommunens politikere, gjerne både i Bystyret og i Bydelsutvalgene.

3. Personvernombudet i Oslo kommune

Ny personopplysningslov trådte i kraft 20. juli 2018.[1] Med denne loven ble også EUs forordning om vern av fysiske personer i forbindelse med behandling av personopplysninger mv. (GDPR – Personvernforordningen) gjort til norsk lov.[2] Det følger av forordningens artikkel 37 at Oslo kommune er forpliktet til å utpeke et personvernombud for kommunen.

Oslo bystyre vedtok i møte 20. juni 2018 å etablere et personvernombud i tråd med kravene i forordningen.[3] Videre ble det besluttet at ombudet skulle etableres som en uavhengig funksjon og plasseres organisatorisk under bystyret.

På bakgrunn av bystyrets vedtak om etablering av personvernombud fremla byrådet sak om mandat for ombudet. Bystyret vedtok mandatet 14. november 2018.

Personvernombud ble ansatt våren 2019 etter en bred rekrutteringsprosess. Morten Haug Frøyen tiltrådte åremålet som personvernombud 13. mai 2019.

Denne årsrapporten gjelder perioden fra 1. januar 2021 til årsskiftet 2021/2022.

4. Personvernombudets mandat

Peker til fullstendig mandat:

https://www.oslo.kommune.no/getfile.php/13314941-1551171862/Tjenester%20og%20tilbud/Politikk%20og%20administrasjon/Etater%2C%20foretak%20og%20ombud/Personvernombudet/Mandat%20for%20personvernombudet%20i%20Oslo%20kommune.pdf

[1] Lov 15. juni 2018 nr. 38 om behandling av personopplysninger (personopplysningsloven).
[2] 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) [GDPR].
[3] Sak 232/2018

5. Personvernombudets oppgaver

Personvernombudets oppgaver, jf. mandatet og personvernforordningen art. 38 nr. 4 og art. 39:

• Informere og gi råd til de behandlingsansvarlige og de ansatte som utfører behandlingen, om de forpliktelsene de har i henhold til personvernregelverket.

• Kontrollere overholdelsen av personvernregelverket og den behandlingsansvarliges personvernretningslinjer, herunder fordeling av det daglige ansvaret for personvernarbeidet i Oslo kommune, holdningsskapende tiltak og opplæring av ansatte som behandler personopplysninger, og tilhørende revisjoner.

• På anmodning, gi råd om vurderinger av personvernkonsekvenser og kontrollere gjennomføringen av vurderingene, i henhold til personvernforordningen art. 35.

• Samarbeide med Datatilsynet.

• Fungere som kontaktpunkt for Datatilsynet ved spørsmål om behandlinger. Dette omfatter forhåndsdrøftingene etter artikkel 36, som må utføres dersom en vurdering av personvernkonsekvenser tilsier at en behandling vil medføre høy risiko som ikke kan reduseres ved tiltak.

• Ved behov, rådføre seg med Datatilsynet om eventuelle andre spørsmål.

• Være tilgjengelig for de registrerte angående spørsmål om behandlingen av deres personopplysninger og om utøvelsen av rettighetene de har i henhold til personvernregelverket.

Arbeidsform og taushetsplikt

Personvernombudet er underlagt taushetsplikt etter personvernregelverket, en plikt som kommer i tillegg til den taushetsplikten som ombudet har etter forvaltningsloven.[4] Denne taushetsplikten er særlig viktig i saker hvor registrerte har spørsmål eller ønsker å varsle om kommunens behandling av registrertes eller andres personopplysninger.

[4] Personopplysningslovens §18: https://lovdata.no/lov/2018-06-15-38/§18

6. Evaluering av personvernombudets organisering og plassering

I Bystyrets møte 20.06.18, sak 232/18 (Byrådssak 146,18) vedtok et enstemmig bystyre at «Organiseringen og plasseringen av personvernombudet evalueres innen to år».[5] Dette var også oppe i et møte i Forretningsutvalget i april 2021.[6] Her ble personvernombudet bedt om å foreta en slik toårs-evaluering.

Personvernombudets åremålsperiode nærmer seg halvveis og det er tidlig å skulle foreta en fullstendig evaluering av ombudets rolle og organisering, ikke minst gitt den spesielle situasjonen vi har vært i de siste årene. En utkvittering av oppdraget vil derfor være delt mellom en vurdering av ombudets organisering og samarbeid (se nedenfor og årsrapporten for øvrig) og informasjon fra fagmiljøets undersøkelse av kompetansebehovet for personvernarbeidet i kommunens virksomheter. Egenevaluering av ombudets arbeid ut over de årlige rapportene har begrenset verdi, rapporter som i seg selv gir innspill og tilbakemeldinger på de områdene som etterspørres. Enkelte forhold vil det uansett være tvilsomt om ombudet selv skal evaluere. Utfordringen med et evalueringsoppdrag reflekterer også at det er viktig og krevende å balansere mellom kravet til ombudets uavhengighet og behovet for å organisere det riktig.

Organisering av ombudet og samarbeid mellom personvernombudet og kommunens virksomheter

I Bystyrets mandat for Personvernombudet stilles det nokså eksplisitte forventinger til informasjonstilgang og involvering:

> 4.4: Informasjonstilgang: Personvernombudet har rett til å få den informasjon som er nødvendig fra alle organer og virksomheter som er en del av Oslo kommune som juridisk person for å utføre sine oppgaver

> 5.3: Involvering av personvernombudet: Personvernombudet skal, på riktig måte og til rett tid, involveres i spørsmål som gjelder vern av personopplysninger. […] Personvernombudet skal informeres om avvik og hendelser i kommunen, herunder hendelser som meldes til Datatilsynet

Hvordan er erfaringene med dette så langt? Organiseringen i Bystyrets sekretariat (BYS) fungerer fint, om enn med noen problemer knyttet til administrative spørsmål som for eksempel opplæring (i Teams, O365 osv) systemskifte og journalføringspraksis. Når det gjelder ombudets behov for informasjon fra kommunens felles løsninger og systemer, er situasjonen mer problematisk. Det er fortsatt nokså

[5] https://tjenester.oslo.kommune.no/ekstern/einnsyn-fillager/filtjeneste/fil?virksomhet=976819853&filnavn=bystyret%2F2018_06%2F1256864_1_1.pdf
[6] https://tjenester.oslo.kommune.no/ekstern/einnsyn-fillager/filtjeneste/fil?virksomhet=976819853&filnavn=5df59460a0eb4e3ea2b755a72d2bc2b5_4ddba05fabc52ed9e299e52c2e38a39a.pdf

store utfordringer knyttet til å få informasjon fra kommunens ulike felles systemer (saksbehandlingssystemer, kvalitetssystemer, osv). Bare møteplanlegging blir en tidstyv for alle parter når ombudet ikke har tilgang til kalendrene til andre ansatte i kommunen (eller omvendt). De systemeiende byrådsavdelingene har ikke vært særlig interessert i å gi ombudet de nødvendige tilgangene. Det dukker stadig opp nye, tekniske utfordringer som er til hinder for informasjonsutveksling. Forklaringene handler som regel om krav til sikkerhet. Det er ikke klart hvorfor dette ikke kan løses.

Overordnet vurdering av kompetansebehovet hos koordinatorene i Oslo kommune

I 2021 gjennomførte FIN/ISI (kommunens sentrale fagmiljø for personvern) en undersøkelse av kompetansebehovet hos de som jobber med personvern i kommunen. En oppsummering av spørreundersøkelser og dybdeintervjuer med personvernkoordinatorer og ledere om kompetansebehovet ble presentert slik (av fagmiljøet for informasjonssikkerhet og personvern) i et kommunalt forum for personvern og informasjonssikkerhet (26.01.22; «Innsikt om læringsbehov hos koordinatorene»):

- Ulike behov for nye koordinatorer og blant de som har vært der en stund
- Topplederne er ikke koblet på arbeidet
- Koordinatorrollen er ikke en fulltidsstilling
- Positive tilbakemeldinger på forum og nettverk – trenger mer av dette
- Ønsker mer rådgivning fra ISI
- Sterkt ønske om at det som kan standardiseres, blir standardisert
- Sterkt ønske om flere maler og verktøy
- Behov for høyere kompetanse hos lederne (kommer fra ledere og koordinatorer)
- Tror at LG/VE-rapporteringen havner i et sort hull
- Informasjonssikkerhet og personvern er ikke en del av styringsdialogen (etterspør fokus på dette)
- Flere sier at de ikke har tatt rollekortene ordentlig i bruk

7. Avvik: Oversikt over brudd på personopplysningssikkerheten[7]

Oslo kommune skal varsle Datatilsynet dersom det har skjedd et brudd på personopplysningssikkerheten i en av kommunens virksomheter med mindre det er usannsynlig at bruddet vil medføre en risiko for de registrertes rettigheter og friheter.

Avviksmeldingen skal blant annet (og som et minimum) inneholde beskrivelse av avviket, mulige konsekvenser, hvilke tiltak som er iverksatt og hvilken informasjon som er gitt til de berørte.

Ombudets avviksoversikt er basert på innhentet informasjon fra Datatilsynet og kommunens virksomheter. Personvernombudet har i for liten grad vært informert om – og involvert i – de ulike avviksmeldingene. Den vedlagte oversikten (vedlegg a) er utarbeidet med utgangspunkt i bistand fra Datatilsynet, som har vært behjelpelig med å ta ut en oversikt over hvilke avvik de kan se å ha mottatt fra Oslo kommune. Det har vært en betydelig forbedring på dette området, men ombudet har tross alt ikke mottatt mer enn litt over halvparten av disse avviksmeldingene direkte fra virksomhetene, til tross at rutiner for dette er tydelig beskrevet i mandatet.[8]

Det er fortsatt mange ledere i Oslo kommune som har en misforstått oppfatning om at antall avvik i egen virksomhet bør være så nær null som mulig. På en del administrative områder (sikkerhet, beredskap, informasjonssikkerhet, personvern osv) har man en tendens til å måle virksomheten etter fraværet av uønskede hendelser. Det paradoksale er at det heller er motsatt. Personvernombudet oppfatter det derfor som positivt at Oslo kommune har en markant økning i antall avvik som ble meldt til Datatilsynet i 2021. Avvik bør oppfattes som en styrke; en vilje til å ta ansvar, se på forbedring, fokusere på kvalitet, vilje til åpenhet og ønske om å hele tiden videreutvikle kommunens tjenester.

«- Hvis du prøver å melde et avvik, så kan du velge adjektiver på øverste hylle: Du er enten en illojal tyster, en patetisk sladrehank eller en kontraproduktiv kranglefant»[9]

[7] Kravet til avviksrapportering er hjemlet i personvernforordningens artikkel 33, nr. 1: Ved brudd på personopplysningssikkerheten skal den behandlingsansvarlige uten ugrunnet opphold og når det er mulig, senest 72 timer etter å ha fått kjennskap til det, melde bruddet til Datatilsynet, med mindre bruddet sannsynligvis ikke vil medføre en risiko for fysiske personers rettigheter og friheter. Dersom bruddet ikke meldes til tilsynsmyndigheten innen 72 timer, skal årsakene til forsinkelsen oppgis.

[8] Oslo kommunes mandat for personvernombudet, pkt. 5.3: «Personvernombudet skal informeres om avvik og hendelser i kommunen, herunder hendelser som meldes til Datatilsynet.»

[9] Samtale med innleid konsulent (tidligere fast ansatt i Oslo kommune) i en av kommunens absolutt ledende digitaliseringsetater

Som vist i tidligere årsrapporter, opplever ombudet fortsatt tendenser til en «fryktkultur» hvor ledere (på alle nivåer) forventer at avvik løses stille og forsiktig og helst skal feies under teppet.

Paradoksalt nok er det ombudets absolutte oppfatning at det er de virksomhetene som melder flest avvik, som gjør den beste jobben på dette området. Halvparten av virksomhetene i Oslo kommune meldte ingen avvik til Datatilsynet i 2021. Det bør gi grunn til ettertanke.

8. Nettverk og samarbeid internt

Ombudet har fortsatt arbeidet med å få på plass samarbeidsformer internt i kommunen.

Personvernombudet har i løpet av 2021 vært i kontakt med de fleste virksomhetene i Oslo kommune. Kontakten har variert fra tett samarbeid og en rekke henvendelser, til et par sporadiske e-poster. Noen eksempler på samarbeid internt i kommunen:

- Bystyrets sekretariat (BYS):
    - Organiseringen med ombudene plassert i Bystyrets sekretariat fungerer godt. Den merkantile støtten innenfor økonomi, arkiv og IT fungerer fint. Det har vært noen utfordringer knyttet til blant annet journalføring og tekniske løsninger.

- Byrådsavdeling for finans/Seksjon for informasjonssikkerhet og IKT (FIN/ISI): Løpende samarbeid og ukentlige møter
    - Ombudet har et tett og godt samarbeid med kommunens sentrale fagmiljø for personvern og informasjonssikkerhet. Samarbeidet foregår løpende fra sak til sak og gjennom ukentlige møter mellom ombudet og fagsjef for personvern. Tilbud i Sikkerhetsmåneden, felles bistand til personvernkonsekvensutredninger i kommunens virksomheter, en mengde enkeltsaker, er noen eksempler på det konkrete samarbeidet.
    - Fagmiljøet og ombudet har fått til et tettere samarbeid med flere byrådsavdelinger og etater etter en risikobasert tilnærming. Dette har ført til faste «trepartsmøter» med byrådsavdelingen for eldre, helse og innbyggertjenester og byrådsavdelingen for oppvekst og kunnskap og faste møter med eksempelvis Helseetaten, Utdanningsetaten osv.

- Utdanningsetaten (UDE): Løpende samarbeid i enkeltsaker, særlig knyttet til henvendelser fra foresatte og ansatte, men også avvikshåndtering, kameraovervåking, snikfilming, publisering av klasselister, utdeling av nettbrett, fotografering, dialog med skoleledere og ansatte osv. Dette samarbeidet har utviklet seg i en særdeles spennende og konstruktiv retning. Bravo!

- Bydelene: Ombudet har vært i dialog med de fleste bydelene i løpet av 2021, om enn i varierende grad. Samarbeidet med bydelene fungerer stort sett godt. Nesten alle bydelene har etablert en funksjon for personvernkoordinator i tråd med rollekortene fra FIN/ISI.[10] De er dedikerte og engasjerte og får gjort

[10] https://felles.intranett.oslo.kommune.no/getfile.php/132424119/%5BFI%5D%20Felles%20intranett/05-Informasjonssikkerhet/Rollekort/Rollekort%20PKO%20v1.0.pdf

imponerende mye på den lille tiden de har fått til rådighet. Litt for ofte er personvernkoordinatorrollen bare nok en oppgave som blir lesset opp i en allerede overfylt portefølje. Det er åpenbart et sterkt behov for øremerking av ressurser knyttet til rollene personvern- og informasjonssikkerhetskoordinatorer (PKO og ISK).

- Plan- og bygningsetaten (PBE): Tett og godt samarbeid knyttet til innbyggerhenvendelser, samarbeid med Dokumentsenteret, personvernkonsekvensutredninger osv.

- Oslo Origo (OO): Faste koordineringsmøter, gjensidig statusrapportering og informasjonsutveksling, fruktbart samarbeid knyttet til digitalisering generelt, avvikshåndtering, personvernvurderinger, kommunale utviklingsprosjekter, osv.

- Helseetaten (HEL): Personvernombudet har vært involvert i en rekke personvernkonsekvensvurderinger, gjennomgang av fagsystemporteføljen, involvering i ulike prosjekter, faste koordineringsmøter og løpende dialog med etaten om en lang rekke koronarelaterte oppgaver og personvernhensynene i disse. Året var – i enda større grad enn 2020 – preget av henvendelser fra bekymrede, frustrerte, provoserte og undrende innbyggere som ønsket mer informasjon og forklaringer knyttet til kommunens løsninger for håndtering av personopplysninger i koronarelaterte systemer (vaksiner, smittesporing, testing, SMS-utsendinger, osv). Takket være godt samarbeid og god oppfølging og utmerket serviceinnstilling fra kollegaer i HEL har innbyggerne fått kvalitetssikrede tilbakemeldinger i løpet av kort tid. Så vidt ombudet har fått tilbakemelding om, har ingen innbyggere følt behov for å gå videre (til Datatilsynet, media, Statsforvalteren eller andre) med sine spørsmål, bekymringer eller innvendinger.

- Sykehjemsetaten (SYE): Tett samarbeid om avvikshåndtering, personvernkonsekvensutredninger og løpende dialog med personvern- og informasjonssikkerhetskoordinatorene

- Barne- og familieetaten (BFE) Brann- og redningsetaten (BRE), Rådhusets forvaltningstjeneste (RFT), Vann- og avløpsetaten (VAV), Bymiljøetaten (BYM), Munchmuseet (MUM), Byarkivet (BYA), Velferdsetaten (VEL) er også eksempler på etater og foretak hvor ombudet har vært involvert i flere saker; det være seg oppfølging av innbyggerhenvendelser, håndtering av avvik, konkret rådgivning til ansatte, ledelsespresentasjoner, vurdering av personvernkonsekvensutredninger, ulike personvernhensyn osv.

En enkel gjennomgang av personvernombudets kalender for 2021 viser at det grovt regnet har vært +/-25 møter i måneden med andre kommunale virksomheter, mens +/-15 møter pr måned har vært med ulike nettverk eller andre, stort sett offentlige, virksomheter. I et spesielt år har så godt som alle møter vært gjennomført på Teams eller andre digitale kanaler.

Personvern i prosjekter – bruk av kommunens data til forskning

En del av personvernombudets rådgivings- og veiledningsfunksjon omfatter kommunens prosjekt- og forskningsvirksomhet hvor det behandles personopplysninger. Dette er blant annet basert på at kommunen er pålagt å involvere personvernombudet i flere prosesser, og at personvernkonsekvensvurderinger i komplekse prosjekter og forskning ofte er omfattende og kompliserte, slik at det er nødvendig med dybdekunnskap og større erfaring.

Personvernombudet gir råd til prosjektledere og forskere både innledningsvis og underveis i prosjekter, gir råd i personvernkonsekvensvurderinger og gir innspill til prosjektenes gjennomføring av personvernkonsekvensvurderinger. Oslo kommune er involvert i mange forskningsprosjekter. Som regel ligger behandlingsansvaret for disse prosjektene hos de ansvarlige forskningsinstitusjonene som har det faglige ansvaret for gjennomføringen. Disse institusjonene har også ansvaret for oppfølgingen av personvernet i prosjektet, men ombudet i kommunen skal være informert og gi råd, tilbakemelding og innspill ved behov. I 2021 (som i 2020) har det vært et 50-talls slike henvendelser, og i alle tilfellene har personvernet tilsynelatende vært godt ivaretatt og involvert aktører som NSD (Norsk senter for forskningsdata), REK (Regionaletisk komité), UiO (Universitetet i Oslo), OsloMET, BI osv.

Fagmiljøet for personvern (FIN/ISI) arbeider med retningslinjer for kommunens krav ansatte skal følge i forbindelse med utlevering av data til bruk i forskning. Ombudet er glad for at dette arbeidet prioriteres og skal sluttføres i 2022.

9. Nettverk og samarbeid eksternt

Henvendelser fra innbyggere i Oslo kommune

Det er et økende antall henvendelser fra kommunens innbyggere (ca. 200 i 2021), noe som likevel fortsatt tyder på at ombudet og ombudets rolle og mandat foreløpig er lite kjent i befolkningen, og at innbyggerne først og fremst benytter seg av førstelinjen i kommunens tjenester når de trenger bistand. Henvendelsene fra de registrerte dekker et bredt spekter. En fellesnevner er at de føler sine rettigheter og friheter krenket, enten på egne vegne eller på vegne av barn eller andre de er foresatte for eller pårørende til. Disse henvendelsene forutsetter et tett samarbeid med de virksomhetene som har eierskap sakene. I 2021 har (igjen) de fleste henvendelsene vært knyttet til korona; dårlig eller mangelfull informasjon, tvil rundt koblinger mot kommersielle aktører, usikkerhet rundt tekniske løsninger, brudd på konfidensialitet for vaksinemotstandere, for å nevne noe.

Innsyn i egne personopplysninger

Noen henvendelser er svært ressurskrevende og involverer samtlige virksomheter i kommunen. Oslo kommune har sin andel av innbyggere som ønsker å kontrollere kommunens arbeid og ønsker å kvalitetssikre de personopplysningene kommunen oppbevarer om dem. Det er veldig fint at noen ønsker å være vaktbikkje, selv om det også kan medføre en del tilsynelatende ressurssløsende ekstraarbeid. Det er et komplisert regelverk som skal håndteres, og det er ikke alltid innbyggerne ser forskjellen på hva man har rett til å få slettet og hva man har en plikt til å dokumentere etter arkiv- og forvaltningslovverket. På dette området er det naturlig å vurdere en revisjon og forenkling av den informasjonen som ligger på kommunens nettsider.

https://www.oslo.kommune.no/personvern-og-informasjonskapsler/innsyn-i-egne-personopplysninger/

UKE har gitt følgende tilleggsinformasjon om skjemaløsningen for begjæring om innsyn i egne personopplysninger i 2021:

«UKE mottar de aller fleste innsynsbegjæringene via skjemaløsningen på OK sine nettsider, men også enkelte fra SvarInn. Henvendelsene registres i WebSak, og det skilles ikke på om de kom fra SvarInn eller skjemaløsningen. UKE mottok 79 henvendelser/innsynsbegjæringer i personopplysninger i 2021.

Sakene fordeles fra arkivet til OKK (Oslo kommunes kontaktsenter), som fordeler dem videre ut i fra informasjonen i innsynsbegjæringen eller informasjon fått i telefonsamtale med begjærer.

OKK sender to svar i hver sak. Ett til innsender med bekreftelse på mottatt henvendelse, og hvor det blir videresendt (hvilke virksomheter). Og ett til virksomhetene det ønskes innsyn fra. Begge svar er etter en mal forfattet av BYR, med noen manuelle tilpasninger. Alt blir sendt ut med samme skjermingsgrad. «Strengt skjermet»

Vi har ikke ført detaljert oversikt (tall e.l.) over hvilke virksomheter i OK som vi videresender innsynsbegjæringer til. Men vi ser at det er innsyn i skolepapirer hos UDE det er mest etterspørsel om når det er en reell innsynssak. Ellers er det gjerne barnevern og barnehjem (Bydeler/BFE/Byarkivet) som blir etterspurt. De fleste spør om innsyn av ren nysgjerrighet, og har ingen klar formening om hvor eller hva de lurer på. Disse snakker OKK med begjærer på telefon, og ender som regel opp med å videresendes til UDE og bydeler, eller at begjæringen trekkes/avsluttes.

UKE har ingen innsikt i det som skjer etter videresending. Det er veldig få oppfølgingssaker inn til UKE vedrørende innsyn.

OKK bruker mest tid på å opprette kontakt med begjærer for å kartlegge behovet/hvor det skal videresendes. Dette gjør at saken kan ligge hos UKE flere dager før videresending.»

I 2022 bør kommunen styrke arbeidet med å koordinere begjæringene om innsyn i egne personopplysninger.

Samarbeid med Datatilsynet

Ombudet har hatt løpende kontakt med Datatilsynet. Kontakten med Datatilsynet har vært hyppig og i form av løpende dialog. I de tilfellene hvor det har resultert i foreløpige eller endelige avviksmeldinger, så er dette dokumentert gjennom de enkelte virksomhetene.

Samarbeid med NAV/Arbeids- og velferdsdirektoratet

Ombudet har hatt regelmessige møter med personvernombudet i Arbeids- og velferdsdirektoratet med gjensidig status, oppdatering og gjennomgang av aktuelle, felles problemstillinger (personvern på NAV-kontorene, delt behandlingsansvar mellom NAVstat og NAVkommune osv). I en del av dette arbeidet har også KS og andre kommuner vært involvert.

Henvendelser fra medarbeidere, fagforeninger, tillitsvalgte og verneombud

I løpet av 2021 merket ombudet en økning i henvendelser fra medarbeidere i Oslo kommune og deres ulike kanaler for medvirkning og samarbeid. Disse henvendelsene kan i hovedsak kategoriseres som bekymring knyttet til ulike former for overvåking i arbeidet. Slik overvåking kan være knyttet til implementering av Office365, detaljert ansattinformasjon på intranett (Workplace, f eks arbeidslister), ulike overvåkningsløsninger ved bruk av sensorer, geolokalisering, flåteovervåking av mobile enheter (EMM), kameraovervåking, filming på ulykkessted eller smitte- eller vaksinestatus for ansatte i ulike virksomheter. Hver for seg har disse systemene og løsningene vært grundig behandlet når det gjelder personvernkonsekvensutredinger og vurderinger av overordnede personvernprinsipper (som formålsavklaring, behandlingsgrunnlag osv) med tilhørende databehandleravtaler og risiko- og sårbarhetsanalyser. Men det er særlig når man ser på hele bildet at man kan gjøre seg refleksjoner knyttet til at omfanget kan bekymre enkelte medarbeidere. Ombudet ser n økende interesse for gråsonene mellom personvern i arbeidslivet og arbeidsrett som

et eget juridisk område. Det er et åpenbart behov for å styrke og forenkle informasjonen, både til medarbeidere og innbyggere.

Nettverk i og utenfor kommunen

Personvernombudet har en særlig uavhengig stilling og er helt avhengig av samarbeid med andre personvernombud for å dele erfaringer, drøfte problemstillinger og samarbeide om beste praksis.

- Nettverk for personvern og informasjonssikkerhet i Oslo kommune (ombudet sitter i programkomitéen, ca. 5 samlinger i året)
- Nettverk for fylkeskommunale personvernombud (løpende samarbeid i Teams, faste møter annenhver uke og kvartalsvise samlinger)
- Nettverk for kommunale personvernombud (samarbeid i LinkedIn og halvårlige samlinger, sitter i programkomitéen)
- Aktiv i Foreningen Personvernombud (ombudet leder valgkomiteen)
- Lokalt nettverk (pvo i Asker, Bærum og Drammen) (løpende samarbeid pr. e-post og samlinger annenhver måned)
- Medlemskap i KiNS (Forum for kommunal informasjonssikkerhet og personvern, ombudet sitter i programkomitéen)
- Nettverk JUC (juridisk nettverk for personvernombud i offentlig og privat sektor)
- Nettverk Advokatkontoret Føyen (nettverk for personvernombud)

10. Noen utvalgte saker

a. Kameraovervåking

Hvor mange overvåkningskamera har Oslo kommune ansvar for? Hvem har overordnet oversikt? Burde det etableres felles retningslinjer på et overordnet nivå for kommunens overvåking? Utdanningsetaten har retningslinjer på vegne av Osloskolen,[11] Deichman Bjørvika, Oslo Havn og andre har gjennomført grundige personvernkonsekvensvurderinger (DPIA) av kameraene på sine områder, men ombudet savner et overordnet bilde av kommunens bruk av overvåkningskamera og ønsker at alle virksomheter får på plass en oversikt (der det ikke allerede finnes) og gjør de nødvendige vurderingene. I 2022 har FIN/ISI satt i gang et arbeid med å lage en juridisk vurdering og retningslinjer til bruk i personvernvurderingene av kommunens kameraovervåking.

b. Overordnede personvernvurderinger for digitale læremidler

For at Osloskolen skal kunne ta i bruk nye digitale læremidler, må disse vurderes for å sikre at de ivaretar elever, lærere og foresattes personvern tilstrekkelig. Personvern handler om retten til et privatliv og retten til å bestemme over egne personopplysninger. Utdanningsetaten har laget en overordnet vurdering av personvern i digitale læremidler (https://aktuelt.osloskolen.no/larerik-bruk-av-laringsteknologi/informasjonssikkerhet-og-personvern/personvern/). Det er også laget vurderinger knyttet til tre av de fire produktgruppene Osloskolen henter tjenester/apper fra; Feide-tjenester,[12] iPad-apper[13] og andre webtjenester[14]. Ombudet har hatt stor nytte av å bli involvert i dette arbeidet. En vurdering av Microsoft-tjenester er under utarbeidelse.

c. «Aktivitetsdata for vurdering og tilpassing (AVT)»

Personvernombudet i Oslo har, sammen med personvernombudet i Bærum, vært involvert i Datatilsynets sandkasseprosjekt (som har vært gjennomført i samarbeid mellom Datatilsynet, KS, Utdanningsetaten og instituttet SLATE ved Universitetet i Bergen). Dette prosjektet har sett på hvordan vi kan gi norske skoleelever individuell vurdering og tilpasset opplæring ved hjelp av læringsanalyse, og samtidig sikre elevene godt personvern? Det har vært spennende diskusjoner særlig knyttet til det rettslige grunnlaget og hvilke konsekvenser et slikt læringsanalysesystem kan ha for

[11] Det er indikasjoner som tyder på at retningslinjene ikke alltid blir fulgt, blant annet er ombudet opptatt av at elever, pårørende og ansatte skal være grundig orientert, involvert og informert i tråd med regelverket for et så inngripende tiltak.

[12] https://aktuelt.osloskolen.no/larerik-bruk-av-laringsteknologi/informasjonssikkerhet-og-personvern/feide-tjenester/

[13] https://aktuelt.osloskolen.no/larerik-bruk-av-laringsteknologi/informasjonssikkerhet-og-personvern/ipad-apper/

[14] https://aktuelt.osloskolen.no/larerik-bruk-av-laringsteknologi/informasjonssikkerhet-og-personvern/andre-webtjenester/

elevenes personvern.[15] Dette er en del av Datatilsynets regulatoriske sandkasse for kunstig intelligens.[16]

d. Bruk av velferdsteknologi i Oslo kommune

Kommunerevisjonen kom høsten 2021 med en rapport knyttet til en forvaltningsrevisjon av Helseetaten og to bydelers arbeid med velferdsteknologi rettet mot innbyggerne i kommunen.[17] Blant anbefalingene i konklusjonen finner vi et ønske om mer informasjon til brukerne:

- brukere, og eventuelt pårørende, får tilstrekkelig informasjon om behandling av personopplysninger i de velferdsteknologiske løsningene.

Personvernombudet vil følge opp dette arbeidet videre, i samarbeid med bydelene og Helseetaten.

e. Fulltekstpublisering

Den europeiske menneskerettighetskonvensjonens artikkel 8 sier: «Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin korrespondanse.» Denne artikkelen samsvarer med vår egen grunnlov som i §102 sier: «Enhver har rett til respekt for sitt privatliv og sitt familieliv, sitt hjem og sin kommunikasjon.» Vår egen Grunnlov føyer til at: «Statens myndigheter skal sikre et vern om den personlige integritet.» Gjennom å bruke ulike offentlige og private søkemuligheter kan man nå kartlegge enkeltpersoner mer enn man kanskje har vært klar over. Her er det viktig at de ansvarlige for personvern er oppmerksomme for faren for å danne seg profiler som til sammen kan gi detaljerte bilder av enkeltinnbyggere.

I 2021 samarbeidet personvernombudet med BLK og Digitaliseringsdirektoratet om problemstillinger knyttet til personvern i forbindelse med utvidelse av kommunens bruk av fulltekstpubliseringsløsningen eInnsyn. FIN/ISI har heldigvis utarbeidet en grundig juridisk vurdering av lovligheten ved en slik publisering. [18]

[15] https://www.datatilsynet.no/regelverk-og-verktoy/sandkasse-for-kunstig-intelligens/ferdige-prosjekter-og-rapporter/avt---sluttrapport/
[16] https://www.datatilsynet.no/regelverk-og-verktoy/sandkasse-for-kunstig-intelligens/rammeverk-for-den-regulatoriske-sandkassen/
[17] https://www.oslo.kommune.no/politikk/budsjett-regnskap-og-rapportering/rapporter-fra-kommunerevisjonen/rapport-15-2021-innforing-av-velferdsteknologi
[18] https://felles.intranett.oslo.kommune.no/getfile.php/132467893/%5BFI%5D%20Felles%20intranett/05-Informasjonssikkerhet/Personvern/Notat%20om%20fulltekstpublisering%20p%C3%A5%20eInnsyn%20v1.0.pdf

f. Personvernerklæringer i Oslo kommune

Noen virksomheter har i 2021 arbeidet med personvernerklæringer rettet mot sin virksomhets behandling av personopplysninger, mens mange nøyer seg med å vise til Oslo kommunes overordnede personvernerklæring.[19] Denne er svært generell og virksomhetene må vurdere spesifikke erklæringer knyttet til de enkelte behandlingene de har ansvar for. Fagmiljøet for personvern og informasjonssikkerhet arbeider med å få på plass et fells malverk og virksomhetene må oppfordres til å kontrollere at dette er på plass, med et klart språk og på et fornuftig nivå.

g. Felles samtykkeløsninger for Oslo kommune

I den grad man er nødt til å bruke samtykke som behandlingsgrunnlag, må slike løsninger være praktisk hensiktsmessige med god tilgangsstyring og med mulighet for aggregering på sikre måter. En sikker løsning må også være praktisk gjennomførbar slik at den fungerer i hverdagen for de som skal bruke den. Ombudet har blant annet vært involvert i arbeidet med Oslo kommunes Mediebank og samtykkeskjemaene som der er rettet mot ansatte, innbyggere og deres eventuelle foresatte og verger.

h. Klart språk

Personvern er et krevende område med stor kompleksitet og tidvis vanskelig tilgjengelighet for andre enn de som jobber tett og mye med fagfeltet. Det er veldig lett for at det utvikler seg et fremmedgjørende stammespråk. Personvernombudet er bekymret for særlig to sider ved kommunens språk på dette området:

- For de ansatte er veiledninger, maler, retningslinjer, rundskriv og annen dokumentasjon lite intuitiv og blir til slutt en ugjennomtrengelig materie for mange.
- For kommunens innbyggere er det ofte vanskelig å tilegne seg den informasjonen som blir sendt ut i ulike kanaler. Datatilsynet setter eksplisitte krav til at vi skal kommunisere med innbyggerne og brukerne av tjenestene våre på en kortfattet, åpen, forståelig og lett tilgjengelig måte.[20] Dette innebærer blant annet:
    - Unngå teknisk eller juridisk sjargong i kommunikasjon om personopplysninger
    - Klart språk, god struktur og lett forståelig informasjon
    - Konkret informasjon
    - Informasjon om behandling av personopplysninger skal være adskilt fra annen informasjon

[19] https://www.oslo.kommune.no/personvern-og-informasjonskapsler/
[20] https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/gi-informasjon/informasjon-og-apenhet/

- Det skal være lett for brukerne å finne fram til riktig og relevant informasjon
- Den enkelte skal ikke ha behov for å sette seg inn i store mengder informasjon for å forstå behandlingen av egne personopplysninger

i. Bekymrede tjenestemottakere og pårørende

Det er grunn til å tro at det er en god del personvernproblematikk knyttet til ulike befolkningsgrupper. Bydelenes begrensede tilgang på personvernressurser harmonerer ikke spesielt godt med det store ansvaret de har for den eldre delen av befolkningen. Personvernombudet har ikke nok innblikk i hvordan personvernprinsippene blir ivaretatt i hjemmetjenestene, i bruken av avansert omsorgsteknologi for demente og andre pleietrengende hjemmeboende, for beboere i omsorgsboliger osv. Arbeidet med en bedre oversikt her må fortsette, i samarbeid med Helseetaten og bydelene.

11. Anbefalinger og videre arbeid

a. Ledelse

Ledere i Oslo kommune har fremdeles en tendens til å gi fra seg ansvaret for personvern og informasjonssikkerhet og ikke innse at dette ansvaret ikke kan delegeres. Ledere i Oslo kommune skal:

- sikre at personvern og informasjonssikkerhet er en del av den helhetlige virksomhetsstyringen
- følge opp medarbeiderne sine (kompetanseheving, kulturbygging, bevisstgjøring)
- stille krav til rapportering og internkontroll
- ha kontinuerlig kontroll i anskaffelser
- sikre tydelig ansvars- og oppgavefordeling

b. Rolleavklaringer

Det må avklares hvem som er ansvarlig for hva. Det er ofte uklart hvem som er systemeier, -forvalter, databehandler osv, og det er ofte uklart hva rollene innebærer. Dette kommer også til uttrykk i arbeidet mellom virksomheter, mellom byrådsavdelinger og mellom byrådsavdelinger og virksomheter. I kommunens overordnede personvernerklæring er dette uklart formulert: «Behandlingsansvarlig er den som bestemmer formålet med behandlingen av personopplysningene. I Oslo kommune er det bystyret som har det overordnede behandlingsansvaret for kommunens behandling av personopplysninger. Det daglige ansvaret er delegert til Oslo kommunes virksomheter.»[21] Dette må utdypes og operasjonaliseres. Toppledelsen i kommunen bør prioritere å følge opp dette så snart fagmiljøets juridiske vurdering for behandlingsansvar er ferdig (i løpet av 2022).

c. Ressurser

Ressurser til personvernarbeid er ikke en engangsutgift som kan reduseres etter hvert som nyhetens interesse kanskje falmer. Personvernarbeid er et kontinuerlig kvalitetsutviklingsløp. Det er et arbeid som krever ressurser i form av både penger og fagfolk. Virksomhetene melder om et betydelig ressursbehov og mangelfull forståelse for at dette ikke er et arbeid som kan sluttstilles eller rett og slett «går over». Alle anskaffelser, all videreutvikling og alle revisjoner av løsninger, behandlinger og prosesser som involverer personopplysninger skal til enhver tid vurderes slik at de tilfredsstiller gjeldende regelverk. For å få til dette på en tilfredsstillende måte, må

[21] https://www.oslo.kommune.no/personvern-og-informasjonskapsler/hvordan-behandler-vi-personopplysningene-dine/

virksomhetene avsette ressurser og kommunen må oppfordre til bedre samarbeid, erfaringsutveksling og deling.

d. Styringssystem for personvern (SSPV)

Oslo kommune har arbeidet for å få på plass et styringssystem for informasjonssikkerhet (SSIS/ISMS). I forlengelsen av dette bør kommunen arbeide for å få på plass et styringssystem for personvern (SSPV).[22] Disse styringssystemene må integreres og ses i sammenheng med kommunens øvrige verktøy.

e. Strategi for digital transformasjon og IKT

Kommunen bør prioritere arbeidet med en strategi for digital transformasjon og IKT. Denne strategien bør se på blant annet

- Reorganisering av digitaliseringsarbeidet i kommunen som helhet, med fokus på tydeligere rolle- og ansvarsfordeling
- Revisjon av Oslo kommunes IKT-reglement

f. Vurdere bruken av sosiale medier (Facebook mm)

Personvernombudet vil anbefale at alle kommunale virksomheter gjør en selvstendig vurdering av hvordan de bruker sosiale medier. Hva slags risiko kan det ha når en virksomhet kommuniserer gjennom Facebook? Og hvilket ansvar for behandlingen av personopplysninger har de? Det er ikke dermed gitt at Oslo kommunes virksomheter skal komme til samme konklusjon som Datatilsynet eller Teknologirådet, som har kommet til at de ikke kan være på Facebook, men det er viktig at man har gjort vurderinger og avveiinger som viser innbyggere, media og andre at man vet hvorfor kommunen bruker de ulike kanalene og de nødvendige risikoreduserende tiltakene er vurdert og eventuelt gjennomført. Dette må ses i sammenheng med generell oppfølging av «overføring til tredjeland»-problematikken (Schrems II-dommen, nye vurderinger fra ulike europeiske datatilsyn, Google Analytics osv)

[22] PIMS (Personal Information Management System – ISO 27701)

g. Avvikshåndtering

Kommunens ledere, det sentrale fagmiljøet for personvern, virksomhetenes personvernkoordinatorer og personvernombudet har en jobb å gjøre for å forbedre håndteringen av mulige og konstaterte brudd på personopplysningssikkerheten i kommunens virksomheter. Vi må bygge en kultur for personvern og etablere rutiner for håndtering av avvik, samtidig som ombudet må involveres tettere i vurderingene om hvorvidt man skal melde et avvik til Datatilsynet eller nøye seg med å dokumentere det i eget kvalitetssystem (for eksempel EQS). Alle ansatte bør bli bedre kjent med kommunens veileder for håndtering av avvik. https://felles.intranett.oslo.kommune.no/informasjonssikkerhet-og-personvern/personvern/veiledninger-og-maler/avvikshandtering-og-melding-til-datatilsynet/

Det var en økning i antall avvik meldt fra Oslo kommune til Datatilsynet fra 2019 til 2020 til 2021; fra 33 avvik i 2019 til 53 innmeldte avvik i 2020, til 98 avvik i 2021.[23] Dette er imidlertid fortsatt et lavt tall og vitner om dårlig vilje til forståelse av kvalitetsarbeid generelt og avvikshåndtering og forbedringsarbeid spesielt. Som en rektor sa: «-Vi kan jo ikke melde inn dette til Datatilsynet, da blir det bare bøter og negativ omtale.» Så kort har vi altså kommet.

24

[23] Dette er omtrentlige tall heftet med stor usikkerhet. Kommunen er langt unna å få på plass et enhetlig avvikssystem med felles rapporteringsrutiner.

[24] Tegneserien «Lunch» av Børge Lund https://www.vg.no/tegneserier/api/images/lunch/2022-02-24.webp

h. Kompetanseheving

Bevisstgjøring, kulturbygging, trygghet og faglig utvikling baserer seg på at medarbeiderne kan lene seg på et faglig fundament og innehar en adekvat mengde med relevant kompetanse. Tilbud om etter- og videreutdanning, «Livslang læring» og en mengde andre honnørord har kommet og gått under ulike regimer og resultatet er at det finnes en myriade av muligheter for den eller de som har lyst, motivasjon, evne, tid og mulighet til å benytte dem. Alt personvernarbeid er nødt til å være risikobasert og derfor er det ikke disse som er i den primære målgruppen for kompetanseheving. Det er de som ikke har tid, lyst, motivasjon, evne, tid og mulighet til å benytte seg av mulighetene som virkelig trenger påfyll.

Kompetansehevingstiltak i Oslo kommune spenner seg over hele spekteret av størrelser og kanaler. Ledere på alle nivåer må få tydelige signaler om at det er deres ansvar å påse at medarbeiderne de har personalansvar for, får tilbud om – og gjennomfører – et minimum av kompetanseheving (små e-postleksjoner eller lignende).

25

26

[25] Tegneserien «Storefri» av Marius Henriksen https://www.vg.no/tegneserier/api/images/storefri/2022-02-27.webp

[26] https://www.vg.no/tegneserier/api/images/storefri/2022-03-11.webp

12. Personvernkonsekvensvurderinger (DPIA)

Fra mandatets pkt. 2.1:
På anmodning, [skal ombudet] gi råd om vurderinger av personvernkonsekvenser og kontrollere gjennomføringen av vurderingene, i henhold til personvernforordningen art. 35.

Ombudet har i arbeidet med personvernkonsekvensvurderingene samarbeidet tett med Byrådsavdelingen for finans (FIN), seksjon for informasjonssikkerhet og IKT (FIN/ISI). Denne seksjonen har et overordnet ansvar for arbeidet med informasjonssikkerhet og personvern i Oslo kommune og har et eieransvar for malverk, veiledninger, prosedyrer og retningslinjer. Dette samarbeidet mellom ombudet, kommunens fagmiljø for personvern og det enkelte prosjektet har fungert veldig bra og vært fruktbart for alle tre parter.

I tillegg er det gjennomført en rekke lokale vurderinger av om det er krav til å gjennomføre en personvernkonsekvensutredning. Dette skjemaet ligger – sammen med øvrig malverk utarbeidet av FIN/ISI – lett tilgjengelig på kommunens intranett.[27] FIN/ISI presenterte et nytt malverk høsten 2021 og dette har blitt godt mottatt i kommunens virksomheter. Det er utarbeidet maler for innledende personvernvurderinger, for personvernkonsekvensvurderinger ved lav/middels risiko og for personvernkonsekvensvurderinger ved høy risiko (DPIA) med vedlegg, sammen med tilhørende veiledninger. Dokumentene er dynamiske og skal revideres og videreutvikles. Blant annet er det et mål å forenkle utfyllingen og å få til et enda enklere og klarere språk, samtidig som de enkelte malene må henge enda bedre sammen, slik at man unngår unødvendig ekstraarbeid.

Arbeidet med vurderinger av personvernkonsekvenser i ulike prosjekter, tjenester og behandlinger forsetter i 2022.

[27] https://felles.intranett.oslo.kommune.no/informasjonssikkerhet/personvern/veiledninger-og-maler/

13. Vedlegg

a. Oversikt over avvik meldt til Datatilsynet i 2021
b. Personvern i Oslo kommune (eksempel på presentasjon for bydelene)
c. Statistikk over gjennomførte e-læringsleksjoner i kommunale virksomheter i sikkerhetsmåneden 2021