

Årsrapport 2020



Personvernombudet
i
Oslo kommune

Innhold

1.	Oppsummering.....	3
	Avvikshåndtering.....	3
	Delingskultur, ressursbruk og tydeligere ansvarsfordeling	3
	Ledelseskultur	4
2.	Definisjoner	5
3.	Personvernombudet i Oslo kommune	6
4.	Personvernombudets mandat.....	7
5.	Personvernombudets oppgaver	7
	Samarbeid med Datatilsynet	8
6.	Oversikt over antall brudd på personopplysningssikkerheten	9
7.	Nettverk og samarbeid internt.....	10
	Personvern i prosjekter	12
8.	Nettverk og samarbeid eksternt.....	13
	Henvendelser fra innbyggere i Oslo kommune	13
	Arbeidsform og taushetsplikt	13
	Nettverk.....	14
	Særlige saker	14
	Schrems II	14
	Fulltekstpublisering	15
	Bekymrede omsorgsboligbeboere og pårørende.....	15
	Skole- og barnehagerelaterte henvendelser fra foresatte:	15
9.	Personvernkonsekvensvurderinger (DPIA/PVK).....	17
10.	Anbefalinger og videre arbeid	19
	Avvikskultur	19
	Delingskultur og bedre ansvarsfordeling.....	19
	Lederkultur	20
	Oversikt over avvik meldt fra Oslo kommune til Datatilsynet 2020.....	22

1. Oppsummering

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/>

Delingskultur, ressursbruk og tydeligere ansvarsfordeling

Et godt personvernarbeid er avhengig av at man evner å heve blikket, tenke helhetlig og samarbeide tett, både på tvers av sektorer og mellom virksomheter. Oslo kommune har en organisering med stor grad av autonomi og delegering av ansvar til de enkelte virksomhetene. På enkelte områder fører det til utfordringer. Hver for seg er personvern og informasjonssikkerhet små elementer i det store kommunemaskineriet. I realiteten fører dette til at kampen om ressursene blir hardere og hardere jo nærmere tjenestemottakerne man kommer. De store etatene har mer ressurser til personvern og informasjonssikkerhet enn mindre virksomheter som for eksempel bydeler, som nødvendigvis prioriterer å levere best mulig tjenester til innbyggerne, noe som samtidig medfører at personvern og informasjonssikkerhet blir tilgodesett med for lite ressurser. Samtidig sitter de sitter isolert i hver sin virksomhet og skal likevel gjøre de samme oppgavene. For å si det enkelt: De sitter for mye på hver sin tue og finner opp hjulet på nytt og på nytt. Det er dårlig utnyttelse av allerede for små ressurser.

Alle virksomhetene i Oslo kommune har etablert koordinatorer for personvern. Det er veldig bra, men koordinatorene har ofte bare en begrenset del av stillingen sin avsatt til dette arbeidet, og det er et åpenbart behov for mer samarbeid på tvers av etatene, virksomhetene og foretakene.

Kommunen må få på plass en helhetlig digitaliseringsstrategi som avklarer ansvarsforholdene bedre enn i dag.

Ombudet opplever at virksomhetenes behov for autonomi og metodefrihet ikke er så stort når det kommer til personvern og informasjonssikkerhet (og andre administrative løsninger i digitaliseringens tid). Da er behovet for standardisering og

en felles metodikk større. Ombudet er opptatt av at alle innbyggere (og ansatte) skal være sikret de samme tjenestene og den samme personvernrettssikkerheten uansett hvor i byen man bor eller hvilken etat man tar kontakt med. Der har kommunen fortsatt en vei å gå. Barnehageområdet har eksempelvis stort behov for koordinering, samarbeid, erfaringsutveksling og tydeligere ansvarsfordeling mellom barnehager, bydeler, etater og byrådsavdeling(er).

Mange virksomheter bruker ekstern kompetanse i større eller mindre grad, også på personvernområdet. Det er ofte riktig og viktig å hente inn slik kompetanse når man ikke besitter den selv, men personvern handler grunnleggende om kulturbygging, og da er det meningsløst å leie inn en ekstern konsulent for å utarbeide en personvernkonsjekvensvurdering som blir liggende i en skuff.

Ledelseskultur

Personvern er et lederansvar. Det skal bygges en kultur og en bevissthet hos alle ansatte hvor personvernet for alle skal utgjøre en ryggmargsrefleks.

2. Definisjoner¹

Brudd på personopplysningssikkerheten (avvik) Hendelse eller situasjon som bryter med gjeldende regler. (Avviksmelding: Sendes til Datatilsynet innen 72 timer)

Behandling av personopplysninger. All bruk av personopplysninger, slik som innsamling, registrering, sammenstilling, lagring og utlevering, eller en kombinasjon av slike bruksmåter.

DPIA (PVK – personvernkonsekvensvurdering). Forkortelse for Data Protection Impact Assessment, en vurdering av personvernkonsekvenser. Dette er en prosess som skal bidra til å håndtere de risikoene behandlingen medfører for enkeltpersoners rettigheter og friheter ved å vurdere dem og fastsette risikoreduserende tiltak.

GDPR. Forkortelse for The General Data Protection Regulation (Personvernforordningen), EUs forordning (regelverk) for personvern.

Personopplysning. Opplysning eller vurdering som kan knyttes til en enkeltperson. Dette kan være navn, adresse, telefonnummer, e-postadresse, bilnummer, bilder eller fødselsdato; «ett eller flere elementer som er spesifikke for nevnte fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sosiale identitet,»²

Sensitive personopplysninger. I loven kalt særlige kategorier av personopplysninger. Dette er opplysninger som krever ekstra vern, slik som opplysninger om rasemessig eller etnisk opprinnelse, religion, helseopplysninger, seksuell orientering med mer.

¹ Se også Datatilsynets ordliste: <https://www.datatilsynet.no/regelverk-og-verktoy/ordliste/>

² Personvernforordningen (GDPR) Art. 4, nr. 1

3. Personvernombudet i Oslo kommune

Ny personopplysningslov trådte i kraft 20. juli 2018.³ 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.⁴ Det følger av forordningens artikkel 37 at Oslo kommune er forpliktet til å utpeke et personvernombud for kommunen fra ikrafttredelsen.

Oslo bystyre vedtok i møte 20. juni 2018 å etablere et personvernombud i tråd med kravene i forordningen.⁵ Videre ble det besluttet at ombudet skulle etableres som en uavhengig funksjon og plasseres organisatorisk under bystyret.⁶

På bakgrunn av bystyrets vedtak om etablering av personvernombud fremla byrådet sak om mandat for ombudet. Bystyret vedtok mandatet 14. november 2018.⁷

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 2020 til årsskiftet 2020/2021.

³ Lov 15. juni 2018 nr. 38 om behandling av personopplysninger (personopplysningsloven).

⁴ 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].

⁵ Sak 232/2018

⁶ Se mer kap. 7: Nettverk og samarbeid internt

⁷ Sak 358/2018

4. Personvernombudets mandat

Peker til fullstendig mandat:

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

Mandatet for personvernombudet i Oslo skal evalueres i 2021/22.

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.

I en stor kommune som Oslo innebærer oppgavene i mandatet et svært omfattende arbeid, og det må nødvendigvis gjøres en del prioriteringer. Det er også løftet frem i mandatets punkt 2.1 at ombudet må prioritere oppgavene basert på ombudets vurdering av risiko.

2020 har vært et spesielt år, også når det kommer til personvern. Ombudets arbeid har like fullt i hovedsak dreid seg om rådgivning til ansatte, bistand ved personvernkonsklusjoner og å være tilgjengelig for de registrerte. Dette betyr at ombudet har vært på «tilbudssiden» og bistått ved behov og vært tilgjengelig for ledere, ansatte og innbyggere i kommunen. Det har altså ikke vært mange saker på ombudets initiativ, men konsultasjoner og henvendelser fra ledere, ansatte og innbyggere som har ført til kontakt og oppfølging med kommunens virksomheter. Koronasituasjonen har naturligvis påvirket arbeidet i stor grad. Mange innbyggere har tatt kontakt med ulike spørsmål om kommunens håndtering av enkeltpersoners helseopplysninger og andre opplysninger av særskilt kategori (art. 9 i Personvernforordningen). Det har også vært en god del henvendelser knyttet til elevers rett til undervisning (særlig i forhold til hjemmeundervisning og strømming av undervisning på gult og rødt nivå).

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.

6. Oversikt over antall brudd på personopplysningssikkerheten⁸

Oslo kommune skal varsle Datatilsynet dersom det har skjedd et brudd på personopplysningssikkerheten i en av kommunens virksomheter og det er sannsynlig at bruddet vil medføre en *risiko* for de registrerte sine 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 1) 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. Ombudet har mottatt bare om lag halvparten av disse avviksmeldingene direkte fra virksomhetene, til tross at rutiner for dette er tydelig beskrevet i mandatet.⁹

Det sentrale fagmiljøet for personvern (FIN/ISI) har i 2020 ledet arbeidet med en veileder for håndtering av brudd på personopplysningssikkerheten og melding til Datatilsynet.¹⁰ Det er viktig at denne veilederen i 2021 blir bedre kjent i kommunens virksomheter.

⁸ 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.

⁹ Oslo kommunes mandat for personvernombudet, pkt. 5.3: «Personvernombudet skal informeres om avvik og hendelser i kommunen, herunder hendelser som meldes til Datatilsynet.»

¹⁰ <https://felles.intranett.oslo.kommune.no/informasjonssikkerhet-og-personvern/personvern/veiledninger-og-maler/avvikshandtering-og-melding-til-datatilsynet/>

7. Nettverk og samarbeid internt

Ombudet har fortsatt arbeidet med å få på plass samarbeidsformer internt i kommunen. Problemene knyttet til uavhengig ombudsorganisering i BYS vs behovet for informasjonstilgang i virksomhetenes fagsystemer (EQS, ACOS Websak osv.) har blitt vesentlig mindre i løpet av 2020.

Personvernombudet har i løpet av 2020 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):
 - o 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. Personvernombudet har faste møter med koordinator for personvern og informasjonssikkerhet i BYS.
- Byrådsavdeling for finans / Seksjon for informasjonssikkerhet og IKT (FIN/ISI): Løpende samarbeid og ukentlige møter
 - o 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, paneldebatt, felles bistand til personvernkonsekvensutredninger i kommunens virksomheter, en mengde enkeltsaker, er noen eksempler på det konkrete samarbeidet.
 - o 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.
- Utviklings- og kompetanseenheten (UKE): Mange ulike samarbeidsområder som for eksempel personvernkonsekvensutredninger, Oslo kommunes kontaktsenter, Kartoteket, avviksarbeid, Google Analytics, forum for meldingsutveksling, flåteovervåkning, KS-samhandling, felles skjema for innsynsbegjæringer for innbyggere forvaltet av UKE, integrasjoner mot det sentrale folkeregisteret osv.
- Byrådsavdelingene (BYR) og Byrådslederens kontor (BLK): Løpende samarbeid, for eksempel knyttet til deltakelse i BYRs forum for personvern og

informasjonssikkerhet, personvernkonsekvensutredninger, avvikshåndtering, fulltekstpublisering osv.

- Utdanningsetaten (UDE): Løpende samarbeid i enkeltsaker, særlig knyttet til henvendelser fra foresatte, men også avvikshåndtering, kameraovervåking, publisering av klasselister, utdeling av nettbrett, fotografering, dialog med skoleledere og ansatte osv. Av alle kommunens virksomheter er nok Utdanningsetaten den med et mest åpenbart ressursbehov på personvern- og informasjonssikkerhetsområdene.
- Bydelene: Ombudet har vært i dialog med samtlige bydeler i løpet av 2020, men i varierende grad. Bydelene Alna, Stovner, Gamle Oslo, Grünerløkka og Søndre Nordstrand er eksempler på bydeler med tett samarbeid med ombudet. Det er initiert et tettere nettverk mellom koordinatorene for personvern og informasjonssikkerhet i bydelene. Ombudet støtter og deltar i dette arbeidet.
- Plan- og bygningsetaten (PBE): Samarbeid knyttet til innbyggerhenvendelser, samarbeid med Dokumentsenteret, personvernkonsekvensutredninger osv.
- Oslo Origo (OO): Faste koordineringsmøter og samarbeid knyttet til digitalisering generelt, avvikshåndtering, kunstig intelligens osv. I forlengelsen av paneldebatten i Sikkerhetsmåneden tok Oslo Origo initiativet til en podcast om personvern, hvor ombudet og en innbygger (som også er en sterk fagperson) samtalte over personvernets begrensninger og muligheter, under profesjonell ledelse av Oslo Origos medarbeider.
- 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 personvern hensynene i disse.
- Sykehjemsetaten (SYE): Tett samarbeid om avvikshåndtering, personvernkonsekvensutredninger og løpende dialog med personvern- og informasjonssikkerhetskoordinatorene
- Kulturetaten (KUL), 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, konkret

rådgivning til ansatte, ledelsespresentasjoner, vurdering av personvernkonsekvensutredninger, ulike personvern hensyn osv.

Personvern i prosjekter

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 personvern vurderinger 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 2020 har det vært et 50-talls slike henvendelser, og i alle tilfellene har personvernet vært godt ivaretatt og involvert aktører som NSD (Norsk samfunnsvitenskapelig datatjeneste), REK (Regionale tisk komité), UiO (Universitetet i Oslo), OsloMET, BI osv.

8. Nettverk og samarbeid eksternt

Henverdeler fra innbyggere i Oslo kommune

Det er fortsatt et lavt (ca. 75) antall henvendelser fra kommunens innbyggere, noe som fortsatt tyder på at ombudet og ombudets rolle og mandat foreløpig er lite kjent i befolkningen, og at de 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. Disse henvendelsene forutsetter et tett samarbeid med de virksomhetene som har ansvar for sakene, både på etats- og virksomhetsnivå.

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 ressursløsende 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.

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

I 2021 bør kommunen styrke arbeidet med å koordinere begjæringene om innsyn i egne personopplysninger.

Arbeidsform og taushetsplikt

Personvernombudet er underlagt taushetsplikt etter personvernregelverket, en plikt som kommer i tillegg til den taushetsplikten som ombudet har etter forvaltningsloven.¹¹ Denne taushetsplikten er særlig viktig i saker hvor registrerte har spørsmål eller ønsker å varsle om kommunens behandling av registrertes eller andres personopplysninger.

¹¹ Personopplysningslovens §18: <https://lovdata.no/lov/2018-06-15-38/§18>

Nettverk

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 og månedsvise møter i programkomitéen)
- 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 etableringen av Foreningen Personvernombud
- Lokalt nettverk (pvo i Asker, Bærum og Drammen) (samarbeid pr. e-post og samlinger annenhver måned)
- Nettverk for personvernombud i offentlige etater (halvårlige samlinger og individuelle møter/e-postsamarbeid)
- Medlemskap i KiNS (Forum for kommunal informasjonssikkerhet og personvern, ombudet sitter i programkomitéen).

Særlige saker

Schrems II

Som et utgangspunkt må man ha et gyldig overføringsgrunnlag etter personvernforordningen for overføring av personopplysninger til tredjeland, altså land utenfor EU/EØS. Sommeren 2020 avsa EU-domstolen den såkalte Schrems II-dommen, som resulterte i strengere krav ved overføring av personopplysninger til tredjeland.

Domstolen kom til at Privacy Shield, som var et overføringsgrunnlag for å overføre personopplysninger til USA, var ugyldig. Begrunnelsen var at USAs lovgivning gir amerikanske myndigheter vide hjemler til å behandle personopplysninger, som strider mot det europeiske personvernregelverket, herunder også den grunnleggende retten til et privatliv som følger av EU-charteret. Privacy Shield har vært et av de mest benyttede grunnlagene for overføring av personopplysninger fra aktører i EU/EØS til USA. Konsekvensen av Schrems II er at all overføring basert på Privacy Shield har vært ulovlig siden Privacy Shield ble vedtatt i 2016. Videre kom domstolen til at EUs standardavtaler (SCC), et alternativt overføringsgrunnlag, var gyldig, men under forutsetning av at partene undersøker om tredjelandet man overfører personopplysninger til gir et tilstrekkelig beskyttelsesnivå for de overførte personopplysningene, og at det innføres ytterligere beskyttelsestiltak dersom dette ikke er tilfellet. Et tilstrekkelig beskyttelsesnivå innebærer at lovgivningen i

tredjelandet gir tilnærmet de samme plikter og rettigheter som etter GDPR. Det samme kravet til ytterligere beskyttelsestiltak vil gjelde også ved bruk av bindende virksomhetsregler (BCR).

Den 11. november 2020 sendte EDPB (det europeiske personvernrådet) to retningslinjer om forståelsen av Schrems II ut på høring. De foreslåtte tiltakene er omfattende, og kommunens sentrale fagmiljø jobber videre med oppfølging av de praktiske konsekvensene av denne dommen for kommunens del.

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.

Bekymrede omsorgsboligbeboere 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 pasient- og brukerombudet og bydelenes personvernkoordinatorer.

Skole- og barnehagerelaterte henvendelser fra foresatte:

- Spørsmål knyttet til mulig krenkelse av enkeltelevs friheter og rettigheter, informasjonsflyt fra skoleledelse, skolehelsetjeneste osv.
- Spørsmål knyttet til mulig krenkelse ifm. trivsels-/mobbeundersøkelser
- Spørsmål knyttet til feilsending av sensitiv informasjon
- Spørsmål fra foresatte om informasjon angående utdeling av nettbrett til barn
- Spørsmål om bruk av robotteknologi i undervisningen (AV1)
- Spørsmål om personvernprinsippene og regelverket knyttet til strømming av undervisning på gult og rødt nivå

- Henvendelser om informasjon og retningslinjer knyttet til fotografering av barn i ulike sammenhenger
- Spørsmål knyttet til sensitiv elevinformasjon på avveie
- Spørsmål om rutiner for ranselpost
- Spørsmål om bruk av apper i skoler og barnehager

Disse henvendelsene er besvart i samarbeid med Utdanningsetaten og byrådsavdelingen for oppvekst og kunnskap (OVK).

9. Personvernkonsekvensvurderinger (DPIA/PVK)

Fra mandatets pkt. 2.1:

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

Personvernombudets involvering i arbeidet med de ulike personvernkonsekvensvurderingene har variert sterkt. På den ene ytterkanten har ombudet vært delaktig hele veien, fra å delta i innledende møter med vurderinger om det foreligger høy risiko for de registrertes rettigheter og friheter, via en prosessorientert arbeidsform med møter og revisjon av ulike utkast fram til ferdig versjon blir oversendt behandlingsansvarlig for avgjørelse. På den andre siden har vi ferdige utkast som blir oversendt ombudet for vurdering og tilbakemelding. Så langt har ikke ombudet bedt om stans eller utsettelse av noen prosjekt. I samarbeid har vi funnet fram til løsninger som har medført at ombudet ikke har hatt grunnleggende innvendinger. Ombudets innspill og tilbakemeldinger har gjennomgående blitt godt mottatt, og endringsforslagene har blitt implementert i vurderingene. Noen av vurderingene har blitt utarbeidet under sterkt tidspress og derfor implisitt stilt krav til ombudets prioriteringer for å unngå at ombudet blir en flaskehals i behandlingen.

En stor variasjon i samarbeidsformene har vært nødvendig ut fra virksomhetenes ulike tilnærminger når det kommer til metodikk, modenhet, kompetanse og ressurstilgang. Dette stiller krav til ombudets fleksibilitet, tilgjengelighet og ombudets evne til å være pragmatisk, konstruktiv og løsningsorientert. Erfaringene så langt har vært gode. Ombudets arbeidsmengde har naturlig nok også variert veldig som en følge av denne bredden, fra et halvt dagsverk til minst et ukesverk pr. vurdering.

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 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. Ikke minst har fagmiljøet fått tilbakemeldinger til bruk i fremtidige revisjoner og endringer i malverk og retningslinjer.

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.¹² Skjemaet presiserer at personvernombudet skal involveres i slike vurderinger. Dette er også et kapasitetsspørsmål, så utover et behov for at ombudet i det minste er orientert, så vil nok etableringen av personvernkoordinatorer i alle virksomheter være

¹² <https://felles.intranett.oslo.kommune.no/informasjonssikkerhet/personvern/veiledninger-og-maler/>

et stort steg i riktig retning. Det sentrale fagmiljøet for personvern har blitt tilført mer ressurser, noe som vil øke deres rådgivningskapasitet.

Arbeidet med vurderinger av personvernkonsekvenser i ulike prosjekter, tjenester og behandlinger forsetter i 2021.

10. Anbefalinger og videre arbeid

Vi skal gjennomføre risiko- og sårbarhetsvurderinger i alle endrings- og utviklingsprosesser, og er vi i tvil om vi bør gjennomføre en personvernkonsekvensvurdering, så skal vi sannsynligvis gjøre det. I det minste skal vi da konsultere ombudet og gå gjennom kommunens mal for å undersøke hvorvidt det foreligger en høy risiko for krenkelse av den registrertes rettigheter og friheter. En slik vurdering skal dokumenteres og er en del av lederansvaret.

Avvikskultur

Det var en økning i antall avvik meldt fra Oslo kommune til Datatilsynet fra 2019 til 2020; fra 33 avvik i 2019 til 53 innmeldte avvik i 2020.¹³ 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.

8 – ÅTTE – bydeler har ikke meldt ett eneste avvik i 2020. Til sammenligning har nokså små kommuner som Nordre Follo og Lindesnes påfallende mange avvik (henholdsvis 21 og 10) i forhold til Oslo. DNB-konsernet har på sin side meldt inn 136 avvik. Det bør være et «mål» for Oslo kommune å ha en kultur som gjenspeiler de reelle avvikene. Slik det er i dag ser vi bare toppen av isfjellet og knapt nok det. Lider kommunen av en fryktkultur hvor man ikke melder avvik av redsel for å bli straffet, gjennom ekstra tiltak uten tilføring av ressurser, kritikk eller noe annet? Kritikken bør komme hvis man ikke tar ansvar og melder fra om avvik man kjenner til.

Kommunens ledere, det sentrale fagmiljøet for personvern og personvernombudet har en stor jobb å gjøre for å bedre rutinene for håndtering av store og små brudd på personopplysningssikkerheten i kommunens virksomheter.

Delingskultur og bedre ansvarsfordeling

Oslo kommune er en stor og kompleks kommune som håndterer en mengde ulike tjenester og har ansvar for en lang rekke systemer. Mange virksomheter samarbeider tett, men etter ombudets oppfatning er det et betydelig potensial for en større delingskultur hvor man deler erfaringer og eksempelvis prosedyrebeskrivelser, retningslinjer, vurderinger, prosesshåndteringer osv., og på den måten styrker en «beste praksis»-tenkning hvor man kan gjenbruke allerede utarbeidede løsninger. Det er fortsatt for mye «silo-tenking» hvor hver enkelt virksomhet sitter hver for seg og gjør mange av de samme oppgavene. Et godt personvernarbeid er avhengig av at man

¹³ Dette er tall heftet med svært stor usikkerhet. Fra Datatilsynets oversikt skal det være meldt inn 7 avvik fra Utdanningsetaten. Etatens egen oversikt viser 19 innmeldte avvik; det er fortsatt ikke høyt, men det er tross alt nærmere en tredobling. For 2021 bør vi klare å finne et tallgrunnlag av bedre kvalitet.

klarer å heve blikket, tenke helhetlig og samarbeide tett, både på tvers av sektorer og virksomheter.

Sett fra personvernombudets side er ansvarsfordelingen i Oslo kommune i beste fall uklar, i verste fall fragmentert. Mangel på helhet og sammenheng gir utydelige ansvarsroller. Personvern (og informasjonssikkerhet) er små hjul i kommunens digitaliseringsarbeid, men må samtidig ses som sentrale elementer i kommunens kvalitetsutviklingsarbeid på alle områder. Kommunen bør klargjøre grensesnittene og ansvarsområdene mellom aktører som FIN/ISI, UKE, BLK, HEL/FSA, Origo og kommunens øvrige virksomheter.

Mange virksomheter bruker ekstern kompetanse i større eller mindre grad, også på personvernområdet. Det er ofte riktig og viktig å hente inn slik kompetanse når man ikke besitter den selv, men personvern handler grunnleggende om kulturbygging, og da er det meningsløst å leie inn en ekstern konsulent for å utarbeide en personvernkonsekvensvurdering.. En slik utredning skal være et dynamisk kulturdokument i en kontinuerlig forbedringsprosess, og det føles meningsløst når ombudet en håndfull ganger får eposter som dette: «- Hei! Takk for spennende og godt samarbeid! Nå er det ikke mer penger igjen og DPIA-en er så godt som avsluttet, så nå er mitt prosjekt i kommunen over for denne gang.» Disse konsulentene opptrer – uten unntak, så langt ombudet kan se – med kommunale e-postadresser. Som et minimum bør kommunen innføre en rutine med at e-postsignaturene skal tilkjenne at det er snakk om innleid kompetanse, ikke ansatte i kommunen. Ombudet har brukt utallige timer på kompetansehevende rådgivning og informasjon til kollegaer som kort tid etterpå har forsvunnet til nye oppdrag.

Lederkultur

Personvern er et lederansvar. Punktum. Alle kommunens ledere må være seg bevisst at lederansvaret blant annet innebærer å

- 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

Veldig mye handler om holdninger hos ledelsen. Personvern må ikke oppfattes som en ekstra byrde og unødvendig ekstraarbeid, men som et fruktbart element i kvalitetsarbeidet. Gjennom å implementere personvernarbeidet i et helhetlig

styringssystem vil både ledere og medarbeidere oppleve større trygghet og bedre kontroll.

Ressursallokering: Ledere må følge opp at alle prosjekt må tilrettelegges med personvernkompetanse helt fra konseptfasen (jf, Digitaliseringsdirektoratets prosjektveiviser: konsept – planlegge – gjennomføre – avslutte – realisere).¹⁴ Det er avgjørende at personvernkonsekvensene blir vurdert allerede i konseptfasen. Ombudet (sammen med kommunens sentrale kompetansemiljø for personvern) kan være en rådgiver og sparringpartner i dette arbeidet, men har ikke ressurser til å gå i dybden i hvert enkelt prosjekt. Virksomhetene må sørge for intern kompetanse på informasjonssikkerhet og personvern. Datatilsynet er også grundige med å påpeke at ombudet ikke skal være saksbehandler og ellers være påpasselig med å sikre sin uavhengighet.

¹⁴ <https://www.prosjektveiviseren.no/>

Oversikt over avvik meldt fra Oslo kommune til Datatilsynet 2020

20/04515-1	Melding om avvik - OSLO KOMMUNE BRANN- OG REDNINGSETATEN	30.11.2020
20/04026-1	Melding om avvik - OSLO KOMMUNE BYDEL 1 GAMLE OSLO	15.10.2020
20/00903-1	Melding om avvik - OSLO KOMMUNE BYDEL 10 GRORUD	16.03.2020
20/02563-1	Melding om avvik - OSLO KOMMUNE BYDEL 10 GRORUD	03.06.2020
20/03277-1	Melding om avvik - OSLO KOMMUNE BYDEL 10 GRORUD	21.08.2020
20/03474-1	Melding om avvik - OSLO KOMMUNE BYDEL 10 GRORUD	04.09.2020
20/00269-1	Melding om avvik - OSLO KOMMUNE BYDEL 12 ALNA	24.01.2020
20/04623-1	Melding om avvik - OSLO KOMMUNE BYDEL 14 NORDSTRAND	07.12.2020
20/03744-1	Melding om avvik - OSLO KOMMUNE BYDEL 2 GRUNERLØKKA	24.09.2020
20/00234-1	Melding om avvik - OSLO KOMMUNE BYDEL 4 ST. HANSHAUGEN	23.01.2020
20/00202-1	Melding om avvik - OSLO KOMMUNE BYDEL 8 NORDRE AKER	21.01.2020
20/00495-1	Melding om avvik - OSLO KOMMUNE BYMILJØETATEN	12.02.2020
20/01116-1	Melding om avvik - OSLO KOMMUNE BYMILJØETATEN	09.04.2020
20/01414-1	Melding om avvik - OSLO KOMMUNE BYMILJØETATEN	14.05.2020
20/04622-1	Melding om avvik - OSLO KOMMUNE BYMILJØETATEN	07.12.2020
20/03972-1	Melding om avvik - OSLO KOMMUNE BYRÅDSAVDELING FOR OPPVEKST OG KUNNSKAP	12.10.2020
20/00622-1	Melding om avvik - OSLO KOMMUNE BYSTYRETS SEKRETARIAT	21.02.2020
20/02452-1	Melding om avvik - OSLO KOMMUNE DEICHMAN BIBLIOTEK	26.05.2020
20/03477-1	Melding om avvik - OSLO KOMMUNE DEICHMAN BIBLIOTEK	04.09.2020
20/03969-1	Melding om avvik - OSLO KOMMUNE DEICHMAN BIBLIOTEK	12.10.2020
20/02581-1	Melding om avvik - OSLO KOMMUNE EIENDOMS- OG BYFORNYELSESETATEN	04.06.2020
20/00542-1	Melding om avvik - OSLO KOMMUNE HELSEETATEN	14.02.2020
20/00684-1	Melding om avvik - OSLO KOMMUNE HELSEETATEN	26.02.2020
20/00833-1	Melding om avvik - OSLO KOMMUNE HELSEETATEN	09.03.2020
20/00236-1	Melding om avvik - OSLO KOMMUNE KULTURETATEN	23.01.2020
20/00166-1	Melding om avvik - OSLO KOMMUNE PLAN- OG BYGNINGSETATEN	21.01.2020
20/01012-1	Melding om avvik - OSLO KOMMUNE SPRÅKSENTERET	30.03.2020
20/02567-1	Melding om avvik - OSLO KOMMUNE SYKEHJEMSETATEN	03.06.2020
20/03847-1	Melding om avvik - OSLO KOMMUNE SYKEHJEMSETATEN	02.10.2020
20/04212-1	Melding om avvik - OSLO KOMMUNE SYKEHJEMSETATEN	30.10.2020
20/04617-1	Melding om avvik - OSLO KOMMUNE SYKEHJEMSETATEN	07.12.2020
20/00704-1	Melding om avvik - OSLO KOMMUNE UTDANNINGSETATEN	28.02.2020
20/03520-1	Melding om avvik - OSLO KOMMUNE UTDANNINGSETATEN	08.09.2020
20/03990-1	Melding om avvik - OSLO KOMMUNE UTDANNINGSETATEN	13.10.2020
20/04214-1	Melding om avvik - OSLO KOMMUNE UTDANNINGSETATEN	30.10.2020
20/04611-1	Melding om avvik - OSLO KOMMUNE UTDANNINGSETATEN	05.12.2020
20/03938-1	Melding om avvik - OSLO KOMMUNE UTVIKLINGS- OG KOMPETANSEETATEN	08.10.2020
20/01016-1	Melding om avvik - BOLIGBYGG OSLO KF	30.03.2020
20/03416-1	Melding om avvik - BOLIGBYGG OSLO KF	01.09.2020
20/03525-1	Melding om avvik - BOLIGBYGG OSLO KF	08.09.2020
20/01467-1	Melding om avvik - JORDAL SKOLE	18.05.2020
20/04052-1	Melding om avvik - STOVNER SKOLE	16.10.2020
20/0000	Melding om avvik - Oslo kommune Utdanningsetaten	07.02.2020
20/0000	Melding om avvik - Oslo kommune Utdanningsetaten	27.03.2020

20/0000	Melding om avvik - Oslo kommune Utdanningsetaten	30.03.2020
20/0000	Melding om avvik - Oslo kommune Utdanningsetaten	08.04.2020
20/0000	Melding om avvik - Oslo kommune Utdanningsetaten	17.06.2020
20/0000	Melding om avvik - Oslo kommune Utdanningsetaten	26.06.2020
20/0000	Melding om avvik - Oslo kommune Utdanningsetaten	30.06.2020
20/0000	Melding om avvik - Oslo kommune Utdanningsetaten	24.09.2020
20/0000	Melding om avvik - Oslo kommune Utdanningsetaten	21.10.2020
20/0000	Melding om avvik - Oslo kommune Utdanningsetaten	26.10.2020
20/0000	Melding om avvik - Oslo kommune Utdanningsetaten	06.11.2020
20/0000	Melding om avvik - Oslo kommune Utdanningsetaten	11.11.2020