Oslo

Personvern i korrupsjons-forebyggende arbeid: Hund og katt eller hånd i hanske?

Innlegg for NFFK
01.09.2022

Morten Haug Frøyen,
personvernombud i Oslo kommune

Agenda

1. Innledning:
   - Hva er personvern?
   - Hva og hvem er personvernombudet?
   - Ombudets mandat, myndighet og oppgaver
2. Personvern i anti-korrupsjonsarbeidet, med vekt på:
   - Metodiske valg
   - Formålsbegrensinger
   - Risiko- og sårbarhetsvurderinger
   - Tilgangsstyring
3. Spørsmål, kommentarer, tilbakemeldinger, innspill

Hva er personvern?

- **EMK artikkel 8**
- Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin korrespondanse.

- **Grunnloven § 102**
- Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin kommunikasjon.
- Statens myndigheter skal sikre et vern om den personlige integritet.

Hva er personvern? Noen begrepsavklaringer

- Avvik
- Behandling av personopplysninger
- Personvernkonsekvensvurderinger
- GDPR
- Hva er en personopplysning?
- Hva er en særlig kategori personopplysninger?

Personvernombudets mandat

- 1. Om mandatet

- 2. Personvernombudets oppgaver (jf. 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.

Personvernombudets mandat, forts.

- 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.

Ved utførelsen av oppgavene, skal ombudet ta hensyn til **risikoene** som er forbundet med behandlingsaktivitetene, herunder behandlingens art, omfang, formål og sammenhengene de utføres i.

Personvernombudets mandat, forts.

Noen utvalgte gullkorn:

- *4.3 Uavhengighet*

Personvernombudet kan **ikke bli instruert** om hvordan ombudet skal utføre sine oppgaver. Ombudet kan ikke avsettes, straffes eller på annen måte sanksjoneres for å utføre sine oppgaver.

- *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. Behandlingsansvarlig skal vurdere personvernombudets råd. Dersom kommunens behandlingsansvarlig ikke tar hensyn til rådene fra personvernombudet, skal uenigheten dokumenteres.

Personvernombudet skal **informeres om avvik og hendelser** i kommunen, herunder hendelser som meldes til Datatilsynet.

Personvernombudets mandat, forts

De siste gullkornene…

- *5.4 Samarbeid*

Som operativ behandlingsansvarlig, ligger ansvaret for å etterleve personvernregelverket i de enkelte virksomhetene. Virksomhetene skal samarbeide med personvernombudet når ombudet ønsker det, og virksomhetene skal sikre tilstrekkelig informasjonsutveksling.

Personvernombudet har adgang til å benytte seg av kompetansen som ligger i kommunens fagmiljøer for personvern, herunder det sentrale fagmiljøet for personvern. Fagmiljøene skal samarbeide med ombudet når ombudet ønsker dette.

Lov om behandling av personopplysninger (personopplysningsloven): Kapittel 5. Personvernombud

, § 18: Personvernombudets taushetsplikt

- Personvernombud plikter å hindre at andre får adgang eller kjennskap til det de i forbindelse med utførelsen av sine oppgaver får vite om

    - a) noens personlige forhold

    - b) tekniske innretninger, produksjonsmetoder, forretningsmessige analyser og beregninger og forretningshemmeligheter ellers når opplysningene er av en slik art at andre kan utnytte dem i sin egen næringsvirksomhet

    - c) sikkerhetstiltak etter personvernforordningen artikkel 32

    - d) enkeltpersoners varsling om overtredelser av loven her.

Taushetsplikten gjelder ikke dersom personvernombudet får samtykke fra den opplysningene gjelder, til å legge dem frem, eller dette er nødvendig for gjennomføring av personvernombudets lovpålagte oppgaver.

Taushetsplikten gjelder også etter at personvernombudet har avsluttet tjenesten eller arbeidet. Opplysninger som nevnt i denne paragraf kan heller ikke utnyttes i egen virksomhet eller i tjeneste eller arbeid for andre.

Samarbeidet med virksomhetene, hva kan ombudet bidra med?

- Bli kjent-møter med etater, virksomheter, foretak, andre ombud, bydeler
- Formidle spørsmål og andre henvendelser fra de registrerte
- Vurdere avvik (skal vi avviksrapportere til Datatilsynet eller skal vi nøye oss med å melde det i våre interne kvalitetssystemer?)
- Planlegge/vurdere/evaluere/bistå i arbeid med personvernkonsekvensutredninger (DPIA/PVK)
- Hjelpe til med å lete etter informasjon
- Følge opp ulike retningslinjer
- Være sparringpartner

Personvern og korrupsjonsforebyggende arbeid – noen problemstillinger

- (kan være) Svært inngripende
- Fokus på formålsbegrensing, tjenestelige behov og behandlingsansvar
- Metodiske valg
- Minimering: (Innsamling: Kjekt å ha eller MÅ ha?)
  - Samle inn så mye som mulig eller satse på stikkprøver?
  - Begynne omfattende eller begynne lavt og heller eskalere?
  - Nødvendighets- og proporsjonalitetsvurdering
  - Informasjonsinnsamling: Hvem kan se hva?
  - MS Office 365 tilbyr en oase av overvåkingsmuligheter! ☹
  - Alltid: Grundige vurderinger i forkant (DPIA)

Grunnleggende huskeliste for personvern

- Innledende personvernvurdering → personvernvurdering ved lav/middels risiko
- Databehandleravtale
- ROS-analyse (risiko- og sårbarhetsvurdering)

→ Full personvernkonsekvensutredning (DPIA)

Grunnleggende personvernprinsipper

1. Behandlingen må være lovlig, rettferdig og gjennomsiktig
2. Formålsbegrensning
3. Dataminimering
4. Riktighet
5. Lagringsbegrensning
6. Integritet og konfidensialitet
7. Ansvarlighet

Tilgangsstyring, tilgangsstyring og atter tilgangsstyring

- Rutiner for kontinuerlig oppdatering av tilgangene til alle ansatte i Oslo kommune (hver natt)
- Oppdaterte systemer
- Oppdaterte ledere….
- (Kort orientering om UKEs tilgangsstyringsprosjekt):

Bakgrunn

- Oslo kommune har i dag to større og flere mindre driftsmiljøer/IKT-plattformer, som alle har sine etablerte verktøy og løsninger for styring av tilganger til IKT-baserte verktøy.
- Oslo kommunes eksisterende tilgangsstyringssystem (PRK) er en eldre løsning som per i dag fremstår med en del teknisk gjeld og et betydelig etterslep på funksjonalitet sammenlignet med kommersielle verktøy for tilgangsstyring
- I UKEs tildelingsbrev for 2020 skal UKE «utrede, planlegge og starte innføring av ny IAM-løsning». Bestillingen konkretiseres ytterligere gjennom oppdragsbrev for ny løsning for tilgangsstyring, mottatt av UKE i april 2020.

Anbefalinger

- Fokusere på endring i arbeidsoppgaver og holdninger når nytt system etableres
- Den nye tilgangsstyringsløsningen må ikke bli «PRK 2.0»
    - Virksomhetene burde ikke videreføre eksisterende arbeidsmetodikk
    - Fokusere på holdningsendring
    - Etablere sentrale retningslinjer
- Opplæring innen tilgangsstyring, informasjonssikkerhet og personvern
    - Sentralt styrt e-læring, nano-kurs
- Tydelig kommunikasjon om fordelene med «En Oslo kommune»
    - Etablere en sterkere enhetsfølelse i Oslo kommune

Kvalitetssikring av anskaffelsesrutiner

- Alle løsninger, prosesser, tjenester og systemer (inkludert endringer) som skal behandle en eller annen form for personopplysninger, SKAL gjennomføre en innledende personvernvurdering FØR driftssetting

- Personvern og informasjonssikkerhet SKAL være et element i alle anskaffelser (jf blant annet Digdirs prosjektveiviser)

Digitalisering kan være korrupsjonsforebyggende

- Digi.no 14. august 2022: Digitalisering er den beste medisinen mot korrupsjon
- Digitalisering (økende grad av e-forvaltning) gir større grad av transparens
- Men: Vi kan digitalisere alt vi orker, men vi kan ikke glemme grunnleggende prinsipper som for eksempel:
  - Klart språk tilpasset mottakerne
  - Dokumentasjonsplikten (journalføring)

Kvalitetsutvikling – hele tiden fokus på forbedring

- Personvern, informasjonssikkerhet og korrupsjonsforebygging er tre sentrale tannhjul i kommunens kvalitetsutviklingsarbeid

- Avvikskultur
  - bevisstgjøring
  - Kulturbygging
  - kompetanseheving

Noen eksempler:

- Workplace: Arbeidslister, sykdomsstatus osv?
- Outlook-kalender: Legge inn sykmeldinger og automatisk svar med informasjon?
- Kameraovervåking i kontorlandskap?
- Innsyn i e-post?
- Flåteovervåking av mobiltelefoner?
- Telefon 24.05.22 kl 08.50: Hjelp, kollegaen min snoker!
- E-post 24.05.22 kl 10.17: Hjelp, jeg vil ikke filmes!

Anbefalinger og videre arbeid

1. Avvikskultur («det er positivt å si ifra»)
   - Økning fra 2019 til 2022
   - Store forskjeller mellom virksomhetene
2. Delingskultur
   - Erfaringsutveksling, «Beste praksis»
3. Ressursbruk
4. Ansvarsfordeling
5. Lederkultur
6. …. Ikke glemme å bygge videre på alt det positive som skjer!

Spørsmål?

- https://www.oslo.kommune.no/etater-foretak-og-ombud/personvernombudet/

- mortenhaug.froyen@oslobystyre.no
- personvernombud@oslobystyre.no

- Tlf: 99569717
- Rådhuset: Kontor nr 132, Vestre tårn