

**<Navn på virksomheten>**

**Rapportering for perioden: <01.09.20xx – 31.08.20xx >**

Innhold

[1 Om virksomhetsleders egenerklæring 3](#_Toc106711676)

[1.1 Virksomhetsleders egenerklæring 3](#_Toc106711677)

[1.2 Rapporteringsperiode 3](#_Toc106711678)

[2 Virksomhetsleders egenerklæring 4](#_Toc106711679)

[2.1 Endringer i virksomhetsleders egenerklæring 9](#_Toc106711680)

[3 Utfyllende kommentarer 9](#_Toc106711681)

[3.1 Kommentar til nr. <tall og overskrift> 9](#_Toc106711682)

[3.2 Kommentar til nr. <tall og overskrift> 9](#_Toc106711683)

[4 Spørsmålsliste 10](#_Toc106711684)

[5 Overordnet tiltaksplan 18](#_Toc106711685)

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Godkjent av: |  | | | U.off: |  | Saksbehandler: | |  | | |
| Godkjent dato: |  | | Versjon: |  | Sak- og dokumentnr: | |  | | | |
| Mal – denne versjonen: | | Virksomhetsleders egenerklæring (2022) | | | Erstatter mal: | Virksomhetsleders egenerklæring (2021) | | | Eier: | FIN |

# 1 Om virksomhetsleders egenerklæring

## Virksomhetsleders egenerklæring

Virksomhetsleders egenerklæring er en rapport på status for en avgrenset del av tiltakene i virksomheten for områdene informasjonssikkerhet og personvern. Rapporten sendes til overordnet byrådsavdeling.

Byrådsavdelingen bruker informasjonen til å følge opp tiltak i sektoren og underliggende virksomheter, og for å sørge for betryggende informasjonssikkerhet og personvern i sektoren. En overordnet statusrapport for hver sektor sammenstilles og sendes til byrådsavdeling for finans.

Byråden for finans har det overordnede ansvaret for informasjonssikkerhet og personvern i Oslo kommune. Resultatene for kommunenivå brukes til å gjøre nødvendig prioritering av tiltak på kommunenivå. Spørsmålene i kapittel 4 gir utfyllende informasjon fra virksomhetene.

I Oslo kommunes instruks for informasjonssikkerhet (byrådssak 1105/13) punkt 3.5 er det et krav om at virksomhetene skal ha en egenerklæring over tiltak innenfor informasjonssikkerhet.

*«Kommunens virksomheter skal dokumentere at lokale sikkerhetstiltak for ivaretakelse av informasjonssikkerhet er implementert gjennom utfylling av egenerklæring. Det samme gjelder systemeiere for fellessystemer og sektorsystemer.»*

Egenerklæringen skal gi en overordnet oversikt over hvilke kontrolltiltak virksomheten implementerer. Virksomhetsleders egenerklæring utgjør en avgrenset del av alle tiltak i virksomheten, og fokuserer på overordnet styring og internkontroll.

## Rapporteringsperiode

Rapporteringsperiode er <01.09.2021 – 31.8.2022>.

Avvik fra dette må avtales med egen byrådsavdeling.

Virksomheter som av en eller annen grunn har et avvikende rapporteringsår, må angi dette innledningsvis i sin rapport.

# Virksomhetsleders egenerklæring

| **Nr.** | **Oppfyllelse av krav** | **Status** | | | **Ref. til evt. kommentar i kap. 3** |
| --- | --- | --- | --- | --- | --- |
|  |  |  |
| **1** | **Risikostyring og internkontroll på personopplysnings- og informasjonssikkerhetsområdet**  Virksomheten har etablert og implementert et styringssystem som ivaretar alle relevante krav til personopplysnings- og informasjonssikkerhet. Styringssystemet er tilpasset virksomhetens tjenester, risikonivå og egenart.   (Jf. Instruks for virksomhetsstyring punkt 3.4 og 3.8, Instruks for internkontroll punkt 4 og GPDR art. 32) |  | | |  |
| Styringssystemet er utformet på en måte som sikrer etterprøvbarhet.    (Jf. Instruks for internkontroll 4) |  | | |  |
| **2** | **Organisering av personvern- og sikkerhetsarbeidet**  Virksomheten har en overordnet beskrivelse av hvordan ansvaret for og arbeidet med personvern og informasikkerhetsarbeidet er organisert og en beskrivelse av de viktigste rollene som er involvert.  (Jf. Instruks for informasjonssikkerhet punkt 3.2) |  | | |  |
| **3** | **Roller og ansvar i arbeidet med personvern og informasjonssikkerhet**  Virksomheten har implementert roller og ansvar i tråd med regelverk og styrende dokumenter.  Oslo kommune har utarbeidet veiledende rollekort som er basert på styrende dokumenter og anerkjent praksis på fagområdet. Se felles intranett: <https://felles.intranett.oslo.kommune.no/informasjonssikkerhet-og-personvern/informasjonssikkerhet/styringssystem-og-internkontroll/roller-og-ansvar/> |  | | |  |
| **4** | **Kompetanse**  Lederne i virksomheten sørger for at ansatte har riktig kompetanse og får tilstrekkelig opplæring til å kunne utøve sine oppgaver knyttet til personvern og informasjonssikkerhet.  (Jf. instruks for informasjonssikkerhet 3.4) |  | | |  |
| **5** | **Brukerinstruks**  Virksomheten påser at ansatte gjøres kjent med sitt personlige ansvar for etterlevelse av krav til personvern og informasjonssikkerhet.  (Jf. instruks for informasjonssikkerhet punkt 3.4 og 5.1) |  | | |  |
| **6** | **Informasjonsoversikt**  Virksomheten har en dokumentert oversikt over hvilken informasjon virksomheten forvalter.  (Jf. instruks for informasjonssikkerhet punkt 4.2) |  | | |  |
| **Informasjonsverdier**  Virksomheten har verdivurdert informasjonen.  (Jf. instruks for informasjonssikkerhet punkt 4.2) |  | | |  |
| **7** | **Oversikt over behandling av personopplysninger**  Virksomheten har dokumentert og oppdatert oversikt over sine behandlinger av personopplysninger iht. personvernregelverket.  (Jf. GPDR art. 30) |  | | |  |
| **8** | **Databehandleravtaler**  Virksomheten (behandlingsansvarlig) har inngått databehandleravtaler med andre (databehandler) som behandler personopplysninger på vegne av virksomheten.  (Jf. GDPR art. 28) |  | | |  |
| **Ordning/avtale om felles behandlingsansvar**  Virksomheten har inngått en ordning/avtale om felles behandlingsansvar der flere virksomheter har felles behandlingsansvar for samme behandling av personopplysninger.  (Jf. GDPR art. 26) |  | | |  |
| **Oversikt over avtaler**  Virksomheten har oversikt over inngåtte databehandleravtaler og ordninger/avtaler om felles behandlingsansvar. |  | | |  |
| **9** | **Rettslige krav**  Virksomheten har oversikt over rettslige forpliktelser som har betydning for ivaretakelse av personvern og informasjonssikkerhet.  (Jf. instruks for informasjonssikkerhet punkt 4.1) |  | | |  |
| **10** | **Risikovurderinger av informasjonssikkerhet**  Virksomheten gjennomfører og dokumenterer risikovurderinger systematisk.  (Jf. instruks for informasjonssikkerhet punkt 3.3 og Instruks for internkontroll punkt 4.2) |  | | |  |
| **Risikohåndtering**  Resultatene av risikovurderingene er sentrale for valg av tiltak for å ivareta konfidensialitet, integritet og tilgjengelighet. Besluttede tiltak følges opp.  (Jf. instruks for internkontroll punkt 4.3) |  | | |  |
| **DPIA**  Virksomheten gjennomfører og dokumenterer vurdering av personvernkonsekvenser (DPIA) for å ivareta de registrertes rettigheter og redusere personvernrisiko.  (Jf. GDPR art. 35) |  | | |  |
| **11** | **Ledelsens gjennomgang**  Virksomheten gjennomfører ledelsens gjennomgang av personvern og informasjonssikkerhet minimum årlig.  (Jf. instruks for informasjonssikkerhet punkt 3.6) |  | | |  |
| **12** | **Utviklingsprosjekter og anskaffelser**  Virksomheten stiller gode og relevante personvern- og sikkerhetskrav i anskaffelser på IKT-området. Det foretas risikovurderinger og personvernkonsekvensvurderinger i forkant av anskaffelsene og underveis, og det blir utført sikkerhetstest og leverandørvurderinger der det er relevant.  (Jf. instruks for informasjonssikkerhet punkt 5.5 og GDPR art. 25.) |  | | |  |
| **13** | **Hendelses-/avvikshåndtering**  Virksomheten har dokumenterte rutiner for intern varsling, rapportering og håndtering av informasjonssikkerhetshendelser og brudd på personopplysningssikkerheten.  (Jf. instruks for informasjonssikkerhet punkt 5.6 og GDPR art. 33-34) |  | | |  |
| Virksomheten har dokumenterte rutiner for at hendelser som kan ha betydning for kommunens felles infrastruktur og/eller internleverandørs drift av systemer, meldes til Utviklings- og kompetanseetaten.  (Jf. instruks for informasjonssikkerhet punkt 5.6) |  | | |  |
| Virksomheten har dokumenterte rutiner for melding av alvorlige informasjonssikkerhetshendelser til overordnet byrådsavdeling, byrådsavdeling for finans, og til aktuelle tilsynsmyndigheter. |  | | |  |
| Virksomheten har dokumenterte rutiner for melding av brudd på personopplysningssikkerheten til overordnet byrådsavdeling, byrådsavdeling for finans, personvernombudet og aktuelle tilsynsmyndigheter, samt for underretning til de registrerte.  (Jf. GDPR art. 33-34) |  | | |  |
| **14** | **Tilgangsstyring**  Virksomheten sikrer at tilgang til informasjon og systemer er i samsvar med tjenstlige behov.  (Jf. Instruks for informasjonssikkerhet, punkt 5.3 og GDPR art. 24) |  | | |  |
| **15** | **Kontinuitetsplanlegging**  Virksomheten har planer for å håndtere situasjoner som kan gi avbrudd i kritisk tjenesteproduksjon.  (Jf. Instruks for informasjonssikkerhet, punkt 5.7 og GDPR 32.) |  | | |  |

## Endringer i virksomhetsleders egenerklæring

Status på følgende punkter i virksomhetsleders egenerklæring er endret:

| **Nr.** | **Betegnelse** | **Status 2021** | | | **Status 2022** | | | **Kommentar** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |
| **1** |  |  | | |  | | |  |
| **2** |  |  | | |  | | |  |

# Utfyllende kommentarer

## Kommentar til nr. <tall og overskrift>

## Kommentar til nr. <tall og overskrift>

# 

# Spørsmålsliste

For at byrådsavdeling for finans skal kunne gi et totalbilde av status for personvern og informasjonssikkerhet i Oslo kommune, må virksomhetsledelsen besvare følgende spørsmål. Spørsmålene relaterer seg til områdene i kapittel 2.

Spørsmålene skal besvares ut fra aktivitet i rapporteringsperioden og status på rapporteringstidspunktet.

**Til område 2, Roller og ansvar:**

|  |  |
| --- | --- |
| **Spørsmål** | **Svar (sett inn tall),  i rapporteringsperioden:** |
| Hvor mange ansatte har virksomheten? |  |
| Hvor mange personer i virksomheten har dedikerte oppgaver innen informasjonssikkerhet og personvern i tillegg til personvernkoordinator (PKO) og informasjonssikkerhetskoordinator (ISK)? |  |
| Hvor mange dedikerte årsverk (én desimal) legger virksomheten ned i informasjonssikkerhet og personvern? |  |
| **Kommentar:** | |

**Til område 4, Kompetanse:**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Spørsmål:**  Har virksomhetene systematikk for å planlegge og gjennomføre kompetanseaktiviteter innenfor informasjonssikkerhet og personvern?  (Her skal virksomhetene svare på om de har egne planer, som går ut over fellesaktiviteter i form av e-læringer og kompetansetilbud i sikkerhetsmåneden) | **Svar (sett kryss):** | **Ja** | | | **Nei** | | | |
|  | | |  | | | |
| Har virksomheten gjennomført opplæring innen informasjonssikkerhet og personvern i rapporteringsperioden? |  | **Ja, for alle** | | **Nei** | | | **For noen** | |
| **For nyansatte** |  | |  | | |  | |
| **Tilpasset ansattes arbeids-oppgaver** |  | |  | | |  | |
| **Tilpasset ledere** |  | |  | | |  | |
| **Har virksomheten ansatte som har tilstrekkelig kompetanse innen områdene (sett kryss):**  Her skal virksomheten svare på om de har kartlagt behov for spesialkompetanse, og har ansatte som fyller behovet. Listen er ikke uttømmende, bruk kommentarfeltet dersom det er andre kompetanseområder som er relevante |  | **Ja** | **Nei** | | | **Ikke rele-vant** | | **Har ikke kart-lagt behov** | |
| **Juridisk kompetanse innen personvern** |  |  | | |  | |  | |
| **Teknisk sikkerhetskompetanse** |  |  | | |  | |  | |
| **Kompetanse på risikovurderinger** |  |  | | |  | |  | |
| **Kommentar:** | | | | | | | | | |

**Til område 6, Verdivurdering:**

|  |  |  |
| --- | --- | --- |
| **Spørsmål** | **Svar (sett kryss),  i rapporteringsperioden:** | |
| Har virksomheten et metodeverk og en skala for å klassifisere/verdivurdere informasjon? | **Vi har metodeverk** |  |
| **Skala er etablert** |  |
| **Har ikke dette på plass** |  |
| **Kommentar:** | | |

**Til område 7, Oversikt over behandling av personopplysninger:**

|  |  |
| --- | --- |
| **Spørsmål** | **Svar (Ja/Nei):** |
| Har virksomhetene oppdatert sine behandlingsoversikter i rapporteringsperioden? |  |
| **Kommentar:** | |

**Til område 8, Databehandleravtaler:**

|  |  |
| --- | --- |
| **Spørsmål** | **Svar (sett inn tall):** |
| Hvor mange databehandleravtaler og/eller ordninger/avtaler om felles behandlingsansvar mangler i virksomheten i rapporteringsperioden? |  |
| Hvor mange databehandleravtaler og/eller ordninger/avtaler om felles behandlingsansvar har virksomheten som ikke vært revidert i tråd med personvernregelverket? |  |
| **Kommentar:** | |

**Til område 10, Risikovurderinger av informasjonssikkerhet:**

|  |  |
| --- | --- |
| **Spørsmål** | **Svar (sett inn tall):** |
| Hvor mange risikovurderinger har virksomheten totalt utført i rapporteringsperioden? |  |
| Hvor mange virksomhetsspesifikke systemer har blitt risikovurdert i rapporteringsperioden? |  |
| Hvor mange virksomhetsspesifikke systemer har virksomheten systemeierskapet for? |  |
| Hvor mange personvernkonsekvensvurderinger (DPIA) har virksomheten utført i rapporteringsperioden? |  |
| Hvor mange personvernkonsekvensvurderinger (DPIA) er blitt oversendt Datatilsynet for forhåndsdrøftelse i rapporteringsperioden? |  |
| Har virksomheten etablert rutiner for gjennomføring av personvernkonsekvensvurderinger (DPIA)? |  |
| **Kommentar:** | |

**Til område 12, Anskaffelser:**

|  |  |
| --- | --- |
| **Spørsmål** | **Svar (sett inn tall):** |
| Hvor mange anskaffelser av systemer eller tjenester, der det stilles krav til informasjonssikkerhet og personvern, har virksomheten gjennomført i rapporteringsperioden? |  |
| For hvor mange av disse anskaffelsene har virksomheten foretatt risikovurdering av informasjonssikkerhet og personvernkonsekvensvurdering i forkant av kravstillingen? |  |
| For hvor mange av disse anskaffelsene har virksomheten foretatt risikovurdering av informasjonssikkerhet og personvernkonsekvensvurdering i andre faser? |  |
| For hvor mange av disse anskaffede systemene har man utført sikkerhetstesting? |  |
| **Kommentar:** | |

**Til område 13, Hendelseshåndtering:**

|  |  |
| --- | --- |
| **Spørsmål** | **Svar (sett inn tall:** |
| Hvor mange avvik og hendelser, som angår informasjonssikkerhet og personvern, har virksomheten hatt i rapporteringsperioden? |  |
| Hvor mange av disse betegnes som alvorlige eller kritiske? |  |
| Hvor mange ganger har virksomheten meldt avvik til Datatilsynet i rapporteringsperioden? |  |
| Hvor mange av avvikene har medført informasjon til den berørte registrerte? |  |
| Hvor mange av avvikene og hendelsene skyldes kjente feil eller sårbarheter som man ikke har klart å fjerne eller rydde opp i? |  |
| **Kommentar:** | |

# 

**Til område 15, Kontinuitetsplanlegging:**

|  |  |  |
| --- | --- | --- |
| **Spørsmål** | **Svar (sett kryss),  i rapporteringsperioden:** | |
| Har virksomheten, som del av sin beredskapsplanlegging, utarbeidet kontinuitetsplaner for håndtering av større og varige brudd på tilgang til kritiske IKT-tjenester og/eller kritisk informasjon? | **Vi har kontinuitetsplaner for relevante scenarier** |  |
| **Vi arbeider med det** |  |
| **Vi har ikke dette på plass** |  |
| Dersom virksomheten har etablert planer, er det gjennomført øvelse(r) av disse? |  | |
| **Kommentar:** | | |

# Overordnet tiltaksplan

Beskriv hvordan virksomheten planlegger å forbedre status på de områdene i egenerklæringen som er gule eller røde. Fyll ut tiltakene i den overordnede tiltaksplanen under.

| **Nr.** | **Tiltak** | **Ansvarlig** | **Frist** |
| --- | --- | --- | --- |
| **1** |  |  |  |
| **2** |  |  |  |
| **3** |  |  |  |