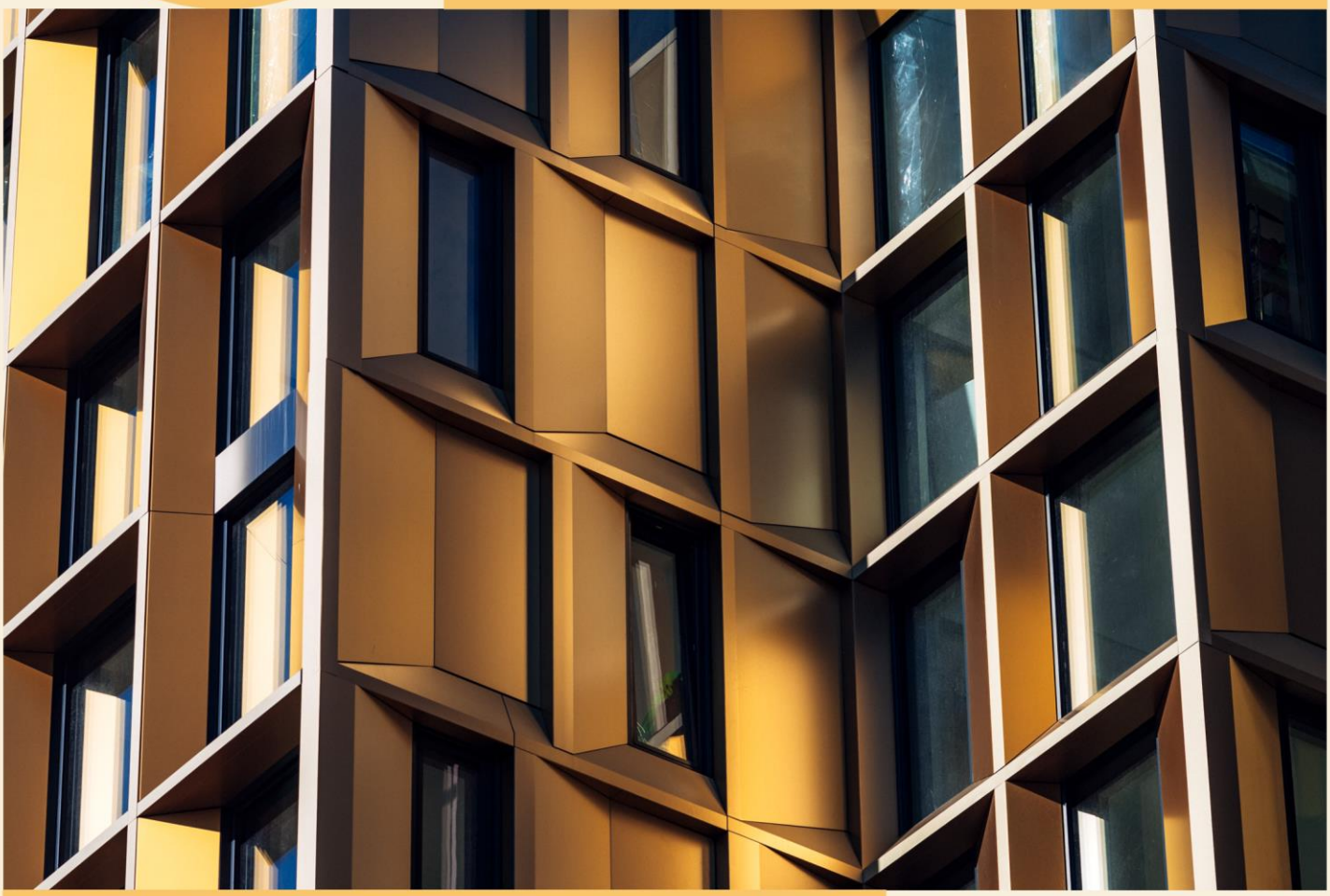
Oslo

Byrådsavdeling for finans

Veiledning

Virksomhetsleders egenerklæring



Virksomhetens overordnede tiltak for styring og internkontroll av informasjonssikkerhet og personvern.

Innhold

Godkjent av:		U.off:		Saksbehandler:	
Godkjent dato:	Versjon:		Sak- og dokumentnr:		
Denne versjonen:	Veileder - Virksomhetsleders egenerklæring (2022)	Erstatter:	Veiledning til Virksomhetsleders egenerklæring (2021)	Eier:	FIN

1 Om virksomhetsleders egenerklæring

A - Virksomhetsleders egenerklæring

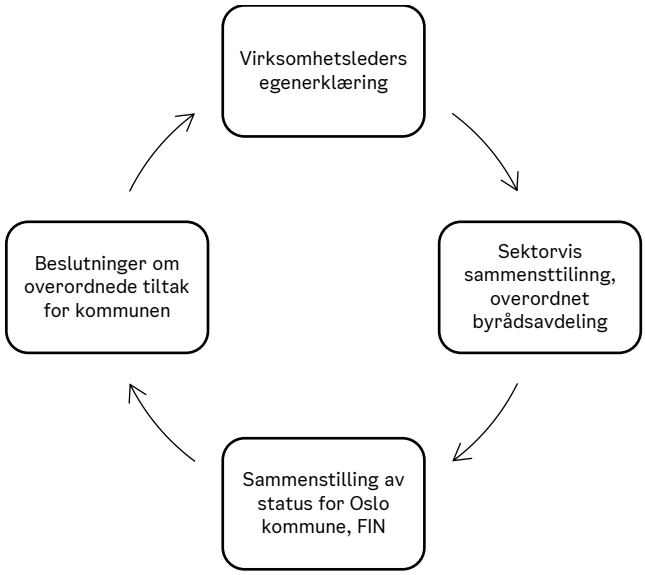
I Oslo kommunes instruks for informasjonssikkerhet (byrådssak 1105/13) punkt 3.5 stilles det krav om at virksomhetene skal ha en egenerklæring over tiltak innenfor informasjonssikkerhet.

«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.

B - Målgruppe for rapporteringen

Målgruppen for Virksomhetsleders egenerklæring er byrådsavdelingen virksomheten hører inn under. 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.



Byrådsavdeling for finans skal ha innsyn i innsendte egenerklæringer for å kunne foreta en oppsummering for Oslo kommune.

Personvernombudet og Kommunerevisjonen kan be om å få innsyn i innsendte egenerklæringer.

Byrådsavdeling 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.

C - Om beskrivelse av funn og tiltak

Rapportene fra Virksomhetsleders gjennomgang vil være unntatt offentlighet. For dette året må vi anta at rapportene blir liggende i Websak+, slik at det vil være ganske bred tilgang for kommunens «innsidere».

Det er vanligvis ikke behov for å presentere detaljert informasjon om funn og tiltak i Virksomhetsleders egenerklæring. Informasjon på et overordnet nivå er tilstrekkelig.

En utdypning av detaljer i funn og tiltak kan avsløre detaljer om virksomhetens sårbarheter og risiko. Utdypning av tiltak avslører sikkerhetstiltakene som implementeres og øker behovet for ytterligere beskyttelse av dokumentet.

D - Om veilederen

Veilederen skal bidra til at Virksomhetsleders egenerklæring blir utarbeidet på en måte som er mest mulig konsistent mellom virksomhetene, slik at det blir enkelt å sammenstille resultatene fra sektor og virksomhetene.

En tilhørende mal som er utarbeidet av Byrådsavdeling for finans (FIN), skal brukes av virksomhetene for selve rapportering.

I denne veilederen finner du beskrivelser av hvordan de ulike kapitlene i malen skal fylles ut.

Kapittel 2 i malen består av 14 ulike områder innen informasjonssikkerhet og personvern, som det skal rapporteres på, og i denne veiledningen finner du forklaring på hva som kreves for å rapportere grønt på de ulike områdene. Kapittel 3 skal inneholde kommentarer til kapittel 2, og kapittel 4 består av spørsmål relatert til de 14 områdene. I kapittel 5 beskrives de overordnede tiltakene for neste rapporteringsperiode,

2 Om malen

A - Slik fyller du ut forsiden

Rapporteringsperioden er satt til 01.09.2021 – 31.8.2022. Avvik fra dette må avtales med egen byrådsavdeling.

- **Fyll inn rapporteringsperiode og navn på virksomheten i boksen på forsiden av rapporten.**
- **Erstatt <Virksomhet> med navn på virksomheten i topptekster.**

B - Slik fyller du ut «2 Virksomhetsleders egenerklæring» i malen

I dette kapittelet fyller virksomheten ut status på de ulike områdene ved å bruke trafikklysmetoden, Grønt, Gult eller Rødt. Som en generell regel kan det sies at:

Grønt	Brukes der virksomheten opplever at de oppfyller kravene det spørres om fullstendig eller i svært stor grad.
Gult	Brukes der virksomheten har et visst samsvar mellom krav og egen praksis. Mangler og avvik er ikke alvorlige, og det skal finnes planer for å oppnå større grad av samsvar.
Rødt	Brukes der det er betydelige mangler og avvik i forhold til kravene det spørres om.

Nedenfor beskrives hva som kreves for å kunne melde grønt på de ulike områdene i kapittel 2 i malen. For å melde gult må virksomheten ha delvis oppfylt kravene til å melde grønt. Som minimum må det finnes overordnede rutiner som er dokumentert og i hvert fall delvis implementert. Et «moderat etterslep» i oppdatering eller bruk av rutinene kan tolereres for fortsatt å melde gult.

2 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)		3.1
	Styringssystemet er utformet på en måte som sikrer etterprøvbarhet. (Jf. Instruks for internkontroll 4)		3.2
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/		3.3

Dersom virksomheten melder gult eller rødt skal det kommenteres i kapittel 3, Oppgi nummer til kommentaren i høyre kolonne «Ref. til evt. Kommentar i kap 3.», slik du ser på bildet.

Område 1: Risikostyring og internkontroll på personopplysnings- og informasjonssikkerhetsområdet :

For å melde grønt på spørsmål a) må virksomheten ha:

- Et styringssystem basert på de til enhver tid gjeldende krav hjemlet i lovverk, besluttede tiltak identifisert i risikovurderinger, besluttet nivå for akseptabel risiko og kommunens føringer innenfor informasjonssikkerhet.
- Et styringssystem som er integrert i driften og oppgaveutførelsen både på strategisk og operasjonelt nivå i henhold til instruks for internkontroll:
    a. På strategisk nivå for å sikre at virksomheten foretar riktige prioriteringer i mål og strategiprosesser og har gode systemer for styring og oppfølging, særlig med tanke på omfattende omstillings- og utviklingsarbeid.
    b. På operasjonelt nivå for å sikre riktige kvalitet i virksomhetens aktiviteter og arbeidsprosesser.
- Prosesser for kontinuerlig forbedring som sikrer at styringssystemet evalueres, kontrolleres og vedlikeholdes med hensyn til effektivitet, hensiktsmessighet og etterlevelse.

For å melde grønt på spørsmål b) må virksomheten ha:

- En oversikt over hva som er nødvendig for å sikre etterprøvbarhet f.eks. årsplaner, dokumentasjon av besluttede tiltak, dokumentasjon av ledelsens gjennomgang, rollebeskrivelser, dokumenterte risikovurderinger, risikohåndteringsplaner, dokumentasjon av hendelseshåndtering, strategier, policy'er, rutinebeskrivelser osv.
- Rutiner og prosesser for å sikre dokumentasjon på etterlevelse.

Område 2: Organisering av personvern- og sikkerhetsarbeidet:

For å melde grønt må virksomheten ha god kontroll og detaljert oversikt over roller, ansvarsområder og oppgaver på personverns- og informasjonssikkerhetsfeltet.

- Det finnes skriftlige dokumentasjon for hvordan arbeidet med informasjonssikkerhet er organisert.
- Ansvaret og oppgavene for informasjonssikkerhet og personvern er fordelt på ulike roller i virksomheten.

Område 3: Roller og ansvar:

For å melde grønt må virksomheten ha etablert rollene som kreves på personverns- og informasjonssikkerhetsfeltet.

- Rollene skal være utdelt til personer.
- Ansvaret og oppgavene er fordelt mellom rollene.

- Det er utpekt koordinatorer for informasjonssikkerhet og personvern som har instrukser med definerte plikter og som kjenner disse.

Område 4: Kompetanse:
For å melde grønt må virksomheten føle seg trygg på at ansatte kjenner sine oppgaver og sitt ansvar for informasjonssikkerhet og personvern.

- Dette gjelder både for de som innehar roller knyttet til informasjonssikkerhet og personvern, og for medarbeiderne generelt.
- Ansatte med særlige oppgaver innenfor informasjonssikkerhet og personvern må være kjent med Oslo kommunes styrende dokumenter for informasjonssikkerhet og personvern, og de deltar jevnlig i faglige fora.
- Øvrige ansatte har fått en grunnopplæring som blir vedlikeholdt gjennom aktiviteter i linjen.

Område 5: Brukerinstruks:
For å melde grønt må virksomheten ha:

- dokumenterte instrukser for å gjøre alle ansatte som får tilgang til informasjon som ikke er offentlig, eller som inneholder personopplysninger, må gjøres kjent med sitt personlige ansvar.
- rutiner og prosedyrer for å gjøre de ansatte innforstått med dette ansvaret.

Område 6: Informasjonsoversikt:
For å melde grønt på a) må virksomheten:

- dokumentere og vedlikeholde en oversikt over hvilken informasjon virksomheten forvalter.
- bidra til å holde Oslo kommunes samlete systemoversikt oppdatert og korrekt.

For å melde grønt på b) må virksomheten:

- ha verdivurdert informasjon med tanke på konfidensialitet, integritet og tilgjengelighet.
- Vurderingen skal skje etter en skala som virksomheten har dokumentert.

Område 7: Personopplysninger:
For å melde grønt må virksomheten:

- ha opprettet en oversikt over personopplysninger som den behandler.
- ha rutiner for jevnlig å vedlikeholde oversikten og følge disse.

Oversikten skal omfatte både behandlingen av personopplysninger i datasystemer og manuelle behandlinger av personopplysninger.

Område 8: Databehandleravtaler:
For å melde grønt på spørsmål a) må virksomheten:

- vite at det er inngått databehandleravtaler der det er relevant, for systemer som behandler personopplysninger.
- følge Digitaliseringsdirektoratets mal for databehandleravtaler, eller dersom det brukes databehandlers egen mal, skal denne være gjennomgått slik at virksomheten ivaretar sine rettigheter og plikter på samme måte som i den anbefalte malen.

For å melde grønt på spørsmål b) må virksomheten:

- vite hvilke underleverandører databehandler benytter, og ha hatt innsyn i databehandlernes avtaler med sine underleverandører.
- ha inngått en avtale om felles behandlingsansvar der virksomheten har felles behandlingsansvar med sammen andre virksomheter eller leverandører.

For å melde grønt på spørsmål c) må virksomheten ha:

- en dokumentert oversikt over inngåtte databehandleravtaler og ordninger/avtaler om felles behandlingsansvar.
- prosedyrer og rutiner for å gjennomgå avtalene og sikre at de ikke er utdaterte ved endringer i systemer, kontraktsforhold eller rammebetingelser for øvrig.

Område 9: Rettslige krav:
For å melde grønt må virksomheten ha

- oversikt over alle sine rettslige forpliktelser som har betydning for ivaretakelse av personvern og informasjonssikkerhet, f. eks. personopplysningsloven, sikkerhetsloven, beskyttelsesinstruksen og eventuell spesifikk, relevant lovgivning (f. eks. barnevernlov, opplæringslov).
- Virksomheten må ha innsikt i hvordan de etterlever kravene.

Virksomheter som er omfattet av spesifikk, relevant lovgivning oppfordres til å liste opp disse lovene eller forskriftene i kommentarboksen.

Område 10: Risikovurderinger av informasjonssikkerhet:
For å melde grønt på spørsmål a) må virksomheten:

- gjennomføre og dokumentere risikovurderinger systematisk.

- oppdatere tidligere utførte risikovurderinger
- ha kriterier for sannsynlighet, konsekvens og akseptabel risiko som er vedtatt av virksomhetens ledelse og forstått av de som har ansvar for risikovurderingene.

Dette innebærer at virksomheten kan godtgjøre at den velger ut systemer og områder for risikovurdering etter en helhetlig vurdering.

For å melde grønt på spørsmål b) må virksomheten:

- ha en prosess for å håndtere risikoer / uønskede hendelser som havner i «rød» eller «gul» sone og om nødvendig eskalere til ledelse på riktig nivå.
- ha rutiner for å få forankret tiltak som velges ut på riktig nivå, sette tiltakene inn i en tidsplan, og tildele disse til en utpekt ansvarlig organisasjonsenhet eller rolle som aktivt kan følge opp.
- involvere virksomhetens ledelse, og eventuelt byrådsavdelingen, ut fra vedtatte regler for risikoaksept.

For å melde grønt på spørsmål c) må virksomheten:

- ha systematikk for å gjennomføre og dokumentere overordnete personvernkonsekvensvurderinger for å ivareta de registrertes rettigheter
- gjennomføre DPIA ved behandling av personopplysninger som medfører en høy risiko for personvernet til de registrerte.

Område 11: Ledelsens gjennomgang:
For å melde grønt må virksomheten:

- ha en prosess, minimum årlig, der ledelsen foretar en gjennomgang av hvordan informasjonssikkerhet og personvern ivaretas.
- Virksomhetens leder må involveres og ha ansvar for selve rapporten. Innholdet av gjennomgangen skal tilsvare det som er beskrevet i en mal fra FIN, men organisering og fremstillingsform kan være annerledes.
- Gjennomgangen skal dokumenteres skriftlig og ende opp i et sett av prioriterte oppgaver.

Område 12: Utviklingsprosjekter og anskaffelser:
For å melde grønt må virksomheten:

- ha en full oversikt over sine IKT-avtaler, inkl. avtaler om skytjenester og evt. driftsavtaler utenom Oslofelles.
- ha prosesser for anskaffelse av IKT-systemer og tjenester som sikrer at relevante krav til personvern og informasjonssikkerhet blir stilt.
    - Kravene må sikre relevant nivå for tilgjengelighet, integritet og konfidensialitet av informasjon, ut fra den informasjonen som behandles og kritikaliteten til at systemene.

    - I tillegg må kravene sikre at relevante bestemmelser etter personopplysningsloven er oppfylt. I den grad virksomheten eller noen av deres informasjonssystemer blir omfattet av ny sikkerhetslov, må videre aktuelle krav til anskaffelse av slike systemer ivaretas.
- Virksomheten må vurdere om det er nødvendig å utføre sikkerhetstesting og ha bestillerkompetanse for slik testing dersom det viser seg nødvendig.
    - Testingen skal avdekke at krav til informasjonssikkerhetskrav er implementert, og det skal ved behov være utført inntrengingstester for å se at ikke uønsket tilgang til data oppstår.

For mer bakgrunn til dette området henvises til Kommunerevisjonens rapport 01/2019 – Sikkerhetskrav i IKT-anskaffelser.

Område 13: Hendelseshåndtering:
For å melde grønt på spørsmål a) må virksomheten:

- ha skriftlige rutiner for intern varsling, rapportering (eskalering) og håndtering av informasjonssikkerhetshendelser og brudd på personopplysningssikkerheten.
    - Rutinene må være tilgjengelige og kjent for medarbeiderne og tilpasset deres oppgaver.
    - Det må finnes verktøyer, digitale eller manuelle, for å foreta varslingen.

For å melde grønt på spørsmål b) må virksomheten:

- ha skriftlige rutiner for at hendelser og avvik som kan ha betydning for Oslo Felles infrastruktur og / eller internleverandørs drift av systemer blir meldt til UKE.
    - Rutinene skal være kjent for de ansatte som har roller med tjenstlig behov for å varsle til UKE.

For å melde grønt på spørsmål c) må virksomheten:

- ha skriftlige rutiner for å melde alvorlige hendelser til sin byrådsavdeling og Byrådsavdeling for finans, samt for varsling til personvernombud og informasjon til de registrerte ved personvernbrudd.
- Ha rutiner for alvorlige hendelser/brudd på personopplysningssikkerheten som innebærer varslingsplikt til tilsynsmyndighet (f. eks. Datatilsynet).

Med alvorlige hendelser menes f. eks. delvis eller fullstendig bortfall av kritiske tjenester, fare for liv og helse, eller sensitiv informasjon (f. eks. tilgang til skjermet infrastruktur eller personopplysninger av særlig karakter) på avveie, slik at uautoriserte har eller kan få tilgang.

Område 14: Tilgangsstyring:
For å melde grønt må virksomheten ha:

- Rutiner for å tildele, administrere og slette tilganger i alle systemer som virksomheten eier eller benytter er dokumentert, og følges opp aktivt.
- Tilgangsstyring er erkjent som et lederansvar.
- Det gjøres periodiske kontroller i tillegg de løpende inn- og utmeldingene av systemene.

Område 15: Kontinuitetsplanlegging
For å melde grønt må virksomheten ha:

- En dokumentert plan for å håndtere situasjoner som kan gi avbrudd i kritisk tjenesteproduksjon.

(Jf. Instruks for informasjonssikkerhet, punkt 5.7 og GDPR 32.)

C – Slik fyller du ut «2.1 Endringer i virksomhetsleders egenerklæring»

I kapittel 2.1 i malen oppgis status på hvilke punkter i virksomhetsleders egenerklæring som er endret fra fjoråret. Kommentarfeltet brukes til å forklare hva forskjellen skyldes.

Det kan være flere årsaker til at en vurdering forandrer seg fra det ene året til det andre. En reell endring i status kan naturligvis være årsaken, men endret vurdering kan også komme av at ny kunnskap er tilgjengelig, eller at skalaen brukes annerledes enn tidligere år.

Merk at det ikke gir mening å gjøre denne sammenlikningen for spørsmål 1, siden dette er nytt av året.

- For å legge til flere rader i tabellen i malen, høyreklikker du og velger «Sett inn» – «Sett inn rader under»

Nr.	Betegnelse	Status 2021	Status 2022	Kommentar
12c	Hendelseshåndtering – varsling til Oslo kommune sentralt og til tilsyn			Rutiner er laget og utprøvd i en øvelse.

D – Slik fyller du ut «3 Utfyllende kommentarer» i malen

I dette kapittelet oppfordrer Byrådsavdeling for finans virksomhetene til å gi utfyllende kommentarer til tabellen i kapittel 2. Her kan virksomhetene gi begrunnelser for valget av fargekode på de enkelte spørsmålene.

Det er spesielt ønskelig at byrådsavdelingene får utfyllende informasjon som gjør dem bedre i stand til å oppsummere status for sektoren.

- Kopier overskriften og fyll inn tall på området og overskriften du kommenterer på fra kapittel 2.
- Husk også å fylle inn referansen i tabellen i kapittel 2 i malen. Se bildet som hører til kapittel 2.

3.1 Kommentar til nr. <tall og overskrift>

E – Slik fyller du ut «4 Spørsmålsliste» i malen

Kapittel 4 i malen inneholder en spørsmålsliste, som må besvares av virksomhetsledelsen. Spørsmålene relaterer seg til områdene i kapittel 2. Svarene baseres på aktiviteten i denne rapporteringsperioden og skal hjelpe byrådsavdeling for finans til å danne seg et totalbilde av status for personvern og informasjonssikkerhet i Oslo kommune.

Spørsmålene skal besvares med JA/NEI, kryss eller med numeriske verdier.

Til område 2, Roller og ansvar:

Spørsmålsboks 1: Fyll ut antall ansatte i virksomheten ved rapporteringsårets slutt, heltid + deltid

Spørsmålsboks 2: Fyll ut antall personer som har spesifiserte roller og spesifikke ansvar

Spørsmålsboks 3: Angi hvor mange årsverk disse personene med spesifikke roller og ansvar utgjør.

Til område 4, Kompetanse:

Spørsmålsboks 1: Her skal virksomhetene svare på om de har egne planer, som går ut over fellesaktiviteter i form av e-læringer og kompetansetilbud i sikkerhetsmåneden, sett kryss.

Spørsmålsboks 2: Her skal virksomhetene svare på om de har gjennomført systematisk opplæring ulike målgrupper.

Spørsmålsboks 3: Her skal virksomheten svare på om de har kartlagt behov for spesialkompetanse, og om de har ansatte som fyller behovet. Listen over spesialkompetanse innen informasjonssikkerhet og personvern er ikke uttømmende, så bruk kommentarfeltet dersom det er andre kompetanseområder som er relevante.

Til område 8: Databehandleravtaler

Spørsmålsboks 2: Her skal virksomheten telle opp antall ordninger eller avtaler de har hvor det foreligger felles behandlingsansvar.

Til område 10: Risikovurderinger

Spørsmålsboks 1: Antallet som kal fylles inn her, gjelder alle utførte risikovurderinger av systemer i rapporteringsperioden. Dersom det har vært foretatt relevante risikovurderinger av intern styring eller av prosesser som ikke henviser til spesifikke systemer, skal også disse tas med i dette tallet.

Spørsmålsboks 4: Når virksomheten skal telle opp personvernkonsekvensvurderinger for rapporteringsperioden, skal alle utførte og godkjente vurderinger tas med. Det skal også presiseres hvilke av disse som fremdeles innebærer en høy risiko for den registrerte og som har blitt sendt til Datatilsynet for en forhåndsdrøftelse. I tillegg skal virksomheten vise hvorvidt det er blitt etablert rutiner for gjennomføring av DPIA, herunder hvilke ressurser som skal delta, forankringsprosess med ledelse og personvernombud, samt kriterier for oversendelse til Datatilsynet.

Til område 12: Anskaffelser
Spørsmålsboks 4: Med sikkerhetstesting menes her at virksomheten har fått utført en test av at leveransen oppfyller sikkerhetskravene. For systemer og prosesser som er eksponert mot åpne nett, kan det være nødvendig å foreta en «inntrengingstest» som en del av sikkerhetstesten.

Med personvernkonsekvensvurderinger menes i utgangspunktet vurderinger etter kravene i personvernregelverket, eksempelvis personvernprinsippene, men også de tilfeller hvor man vet risikoen er høy og derfor skal gjennomføre DPIA,

Til område 14, Kontinuitetsplanlegging:

Dette området kom inn i Virksomhetsleders egenerklæring i 2021. Erfaringer fra pandemi og med trusselsituasjonen i Norge og verden, er det besluttet av Byrådsavdeling for finans at det er et behov for å få oversikt over virksomhetenes planer for beredskap og kontinuitet.

F - Slik fyller du ut «5 Overordnet tiltaksplan» i malen

Den overordnete tiltaksplanen skal vise hvordan virksomheten planlegger å forbedre status på de områdene i egenerklæringen som er gule eller røde. Det er ikke nødvendig å gi noen detaljert beskrivelse. Tiltakslisten skal fungere som en huskeliste for hva virksomheten må jobbe mer med, og gjerne som et utgangspunkt for en mer helhetlig tiltaksplan. Tiltaksplanen her bør være konsistent med listene bakerst i Ledelsens Gjennomgang.

- For å legge til flere rader i tabellen i malen, høyreklikker du og velger «Sett inn» – «Sett inn rader under»

Nr.	Tiltak	Ansvarlig	Frist
1	Roller og ansvar: Evaluering av sikkerhetsorganisasjonen og av ISKs oppgaver.	Informasjonssikkerhets-ansvarlig	01.12.2021
2	Rollekort: Gjennomgang av rollekort fra Byrådsavdeling for finans for å vurdere om det er behov for endringer i egen sikkerhetsorganisasjon, eller om det er oppgaver som ikke ivaretas i dagens etablerte roller for å ivareta informasjonssikkerhet.	Informasjonssikkerhets-ansvarlig	01.03.2022
3	Kompetanse: Det skal være etablert plan for kompetansehevende tiltak.	Informasjonssikkerhets-ansvarlig i samarbeid med leder for personalseksjonen	01.06.2022