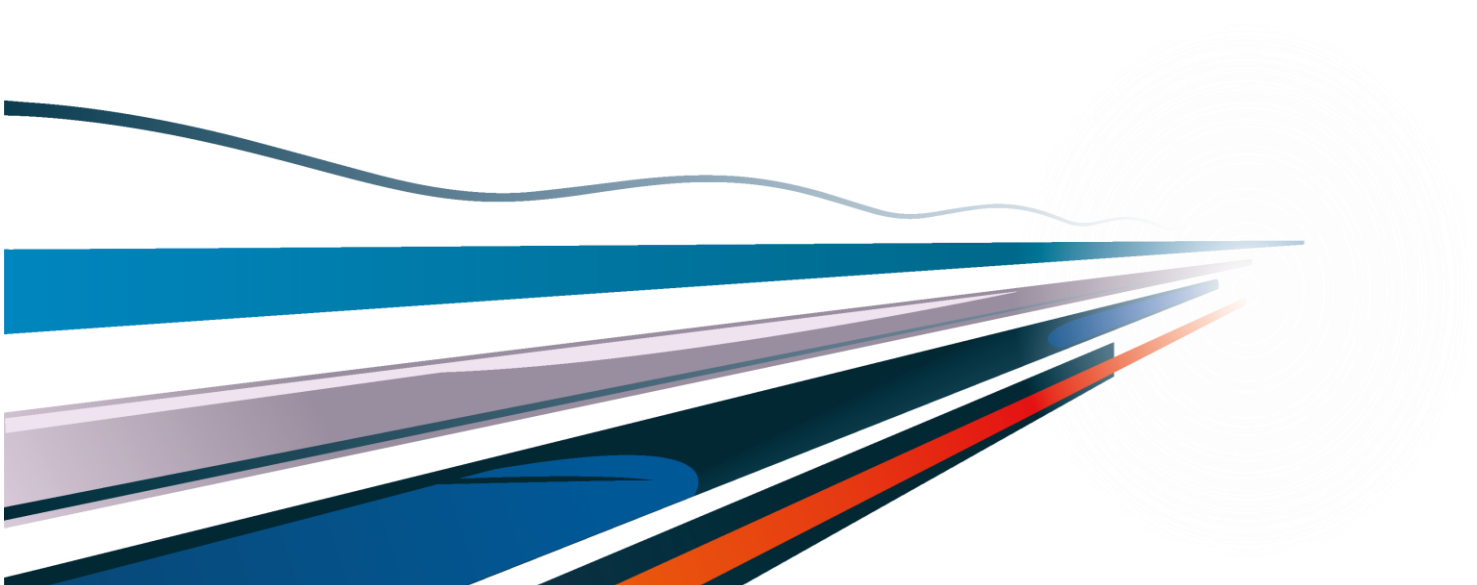




KOMMUNAL- OG  
MODERNISERINGSDEPARTEMENTET

Økonomi- og virksomhetsinstruks  
for  
Datatilsynet

18.12.2019



## Innholdsfortegnelse

<b>1. INNLEDNING</b>	<b>2</b>
<b>2. DATATILSYNETS MYNDIGHET OG ANSVAR</b>	<b>2</b>
2.1 DATATILSYNETS FORMÅL OG TILKNYTNINGSFORM	2
2.2 DATATILSYNETS FORVALTNINGSOMRÅDER	2
2.2.1 FAGORGAN	2
2.2.2 TILSYNSVIRKSOMHETEN	2
2.2.3 OMBUDSROLLEN	3
2.3 REGELVERK SOM REGULERER DATATILSYNETS AKTIVITETER ELLER TJENESTEOMRÅDER	3
<b>3. KOMMUNAL- OG MODERNISERINGSDEPARTEMENTETS STYRING AV DATATILSYNET</b>	<b>3</b>
3.1 DEPARTEMENTETS OVERORDNEDE ANSVAR	3
3.2 STYRINGSDIALOGEN	3
3.2.1 TILDELINGSBREV	3
3.2.2 ETATSSTYRINGSMØTER	4
3.2.3 LEDERLØNNSKONTRAKT OG LEDERLØNSSAMTALE	4
3.2.4 RAPPORTERING GJENNOM ÅRET	4
3.2.5 OPPFØLGING AV SAKER FRA RIKSREVISJONEN	4
3.2.6 ÅRSRAPPORT	4
3.3 KOMMUNIKASJON, ANSVAR FOR AVKLARINGER OG INFORMASJONSPLIKT MELLOM DEPARTEMENT OG VIRKSOMHET	6
3.4 ADMINISTRATIVE FULLMAKTER	7
3.4.1 ANSETTELSE, OPPRETTELSE AV STILLINGER OG LØNNFASTSETTELSE	7
3.4.2 ERSTATNINGSKRAV MOT STATEN	7
3.4.3 ADMINISTRATIVE BESTEMMELSER OM FLYTTING TIL/FRA UTLANDET	7
3.4.4 UTDANNINGSPERMISJON VED STUDIEREISER TIL UTLANDET	7
3.4.5 ARBEIDSGIVERFINANSIERTE ELEKTRONISKE KOMMUNIKASJONSTJENESTER	7
<b>4. DATATILSYNETS INTERNE STYRING</b>	<b>7</b>
4.1 VIRKSOMHETSLEDELSENS MYNDIGHET OG ANSVAR	7
4.1.1 GODTGJØRELSE/ANDRE UTBETALINGER TIL DIREKTØREN	8
4.2 VIRKSOMHETENS INTERNE STYRING	8
4.2.1 RISIKOSTYRING	8
4.2.2 EVALUERINGER	8
4.2.3 ARBEIDSGIVERROLLEN (HMS OG LIKESTILLING)	9
4.2.4 REGNSKAPSPRINSIPP OG REGNSKAPSFØRING	9
4.3 KRAV TIL VIRKSOMHETENS INTERNKONTROLL	9
4.4 VIRKSOMHETENS ARBEID MED SIKKERHET	9
4.4.1 SAMFUNNSSIKKERHET OG BEREDSKAP	10
4.4.2 INFORMASJONSSIKKERHET	10

## 1. INNLEDNING

Instruksen er fastsatt av Kommunal- og moderniseringsdepartementet (KMD) den 18.12.2019, jf. reglement for økonomistyring i staten § 3, andre ledd, og trer i kraft fra 01.01.2020. Kopi av instruksen er sendt til Riksrevisjonen.

Instruksen har som formål å sikre god og forsvarlig økonomi- og virksomhetsstyring i Datatilsynet.

Økonomi- og virksomhetsstyringen i Datatilsynet skal følge Finansdepartementets Reglement for økonomistyring i staten (heretter kalt Reglementet), Bestemmelser om økonomistyring i staten (heretter kalt Bestemmelsene) og rundskriv fra Finansdepartementet, med de tilføyelser og presiseringer som departementet har gitt i denne instruksen. Reglementet, Bestemmelsene og rundskriv fra Finansdepartementet gjelder således i sin helhet, også de punkter som ikke er omtalt i denne instruksen.

Reglementet, Bestemmelsene og rundskriv fra Finansdepartementet er ikke gjengitt i denne instruks.

## 2. DATATILSYNETS MYNDIGHET OG ANSVAR

### 2.1 Datatilsynets formål og tilknytningsform

Datatilsynet er tilsynsmyndighet etter personopplysningsloven § 20 og personvernforordningen artikkel 51 og er et uavhengig forvaltningsorgan administrativt underlagt Kongen og departementet. Datatilsynet kan ikke instrueres om behandling av enkeltsaker eller om den faglige virksomheten for øvrig, jf. personopplysningsloven § 20. Datatilsynets uavhengighet, kompetanse, oppgaver og myndighet er nærmere regulert i personopplysningsloven kapittel 6-7 og personvernforordningen kapittel VI.

Formålet med Datatilsynets virksomhet er å bidra til at personvernlovgivningen etterleves.

Datatilsynet er et ordinært statlig forvaltningsorgan (bruttobudsjettet virksomhet).

### 2.2 Datatilsynets forvaltningsområder

Datatilsynet er fagorgan, tilsyn og ombud på personvernområdet, og skal utføre de oppgaver som fremgår av personvernforordningen artikkel 57 nr. 1. Dette omfatter blant annet, men ikke utelukkende, oppgaver nevnt i pkt. 2.2.1 – 2.2.3.

#### 2.2.1 Fagorgan

Som fagorgan skal Datatilsynet holde seg løpende orientert om utviklingen på personvernområdet. Videre skal Datatilsynet blant annet behandle klager på behandling av personopplysninger, samt gi råd og veiledning om korrekt behandling av personopplysninger til både privatpersoner og virksomheter. Datatilsynet skal også gi faglige råd til departementets utforming av personvernpolitikken og etter nærmere avtale med departementet bistå departementet i fagsaker.

#### 2.2.2 Tilsynsvirksomhet

Datatilsynet skal føre tilsyn med og håndheve anvendelsen av regler om behandling av personopplysninger, jf. personopplysningsloven § 20 tredje ledd, jf. personvernforordningen art. 58.

Kommuneloven §§ 30-6 og 30-7 gir regler om samordning av statlig tilsyn med kommunene. Datatilsynet skal innen 1. desember hvert år underrette fylkesmannen om planlagte tilsyn for kommende år. Datatilsynet skal benytte den nasjonale tilsynskalenderen som driftes av Fylkesmennes fellesadministrasjon. Datatilsynet deltar videre i Arena for nasjonal samordning av tilsyn med kommunene i samsvar med mandat av 30. november 2017. Formålet med arenaen er å legge til rette for at statlige tilsynsmyndigheter kan opptre mer enhetlig overfor fylkesmannen,

kommuner og fylkeskommuner. Samordningsplikten påvirker ikke Datatilsynets tilsynskompetanse og uavhengighet etter personopplysningsloven og personvernforordningen.

### **2.2.3 Ombudsrollen**

Datatilsynet skal fremme allmennhetens kjennskap til og forståelse for personvern, samt fremme personvern som en sentral verdi i samfunnet. I dette arbeidet bør Datatilsynet ta i bruk et bredt spekter av formidlingskanaler og delta i offentlig ordskifte om personvern.

## **2.3 Regelverk som regulerer Datatilsynets aktiviteter eller tjenesteområder**

Datatilsynets virksomhet skal utøves innenfor det regelverk som berører tilsynets aktiviteter og tjenester. Sentralt regelverk er:

- lov om behandling av personopplysninger 15. juni 2018 nr. 38
- lov om Schengen informasjonssystem 16. juli 1999 nr. 66
- lov om helseregistre og behandling av helseopplysninger 20. juni 2014 nr. 43
- lov om behandlingsbiobanker 21. februar 2003 nr. 12
- lov om register over opplysninger om valutaveksling og overføring av betalingsmidler inn og ut av Norge 28. mai 2004 nr. 29
- lov om medisinsk og helsefaglig forskning 20. juni 2008 nr. 44
- lov om behandling av opplysninger i politiet og påtalemyndigheten 28. mai 2010 nr. 16
- forskrift om kameraovervåkning i virksomhet 2. juli 2018 nr. 1107
- forskrift om arbeidsgivers innsyn i e-postkasse og annet elektronisk lagret materiale 2. juli 2018 nr. 1108

## **3. KOMMUNAL- OG MODERNISERINGSDEPARTEMENTETS STYRING AV DATATILSYNET**

### **3.1 Departementets overordnede ansvar**

Statsråden har det konstitusjonelle og politiske ansvaret for Datatilsynet. KMD har det overordnede administrative og budsjettmessige ansvaret for virksomheten. Departementets styringsansvar bygger på prinsippene om mål- og resultatstyring og tar utgangspunkt i departementets overordnede kontrollansvar iht. Bestemmelsene pkt. 1.6.2. Departementets administrative ansvar for Datatilsynet griper ikke inn i tilsynets faglige uavhengighet.

### **3.2 Styringsdialogen**

Styringsdialogen mellom KMD og Datatilsynet skal vektlegge effektiv ressursutnyttelse og virksomhetens resultater basert på de oppgaver tilsynet er pålagt i personvernforordningen artikkel 57 nr. 1, samt risikovurderinger.

Styringsdialogen skal være dokumentert.

#### **3.2.1 Tildelingsbrev**

Etatsstyringen skjer hovedsakelig gjennom tildelingsbrev og etterfølgende oppfølging og rapportering. I tildelingsbrevet formidles Stortingets vedtak og forutsetninger. Tildelingsbrevet inneholder de bevilgninger som stilles til Datatilsynets disposisjon, samt en oversikt over Datatilsynets fullmakter i budsjettåret. Tildelingsbrevet inneholder en styringskalender hvor de viktigste elementene i styringsdialogen det enkelte året fremgår.

Eventuelle endringer i løpet av budsjettåret vil bli formidlet til Datatilsynet i supplerende tildelingsbrev.

### **3.2.2 Etatsstyringsmøter**

Departementet holder som hovedregel ett etatsstyringsmøte med Datatilsynet i løpet av året. Tidspunktet for etatsstyringsmøtet vil fremgå av styringskalenderen. Møtet vil ta utgangspunkt i årsrapport for foregående år, samt planer for inneværende år. Nærmere tema for møtet avklares i forkant. Aktuelle temaer er bl.a. prioritering og gjennomføring av aktiviteter i samsvar med personvernforordningen artikkel 57 nr. 1, gjennomgang av overordnet risikovurdering, budsjettstatus, sikkerhet og eventuelle saker fra Riksrevisjonen. Det skrives referat fra etatsstyringsmøtene.

Utover den ordinære styringen kan det holdes både informasjons- og kontaktmøter av faglig og/eller administrativ karakter mellom departementet og Datatilsynet. Disse møtene er ikke styringsmøter.

### **3.2.3 Lederlønnskontrakt og lederlønnssamtale**

Direktøren utnevnes i statsråd. Departementet utarbeider lederlønnskontrakt.

Departementet innkaller direktøren til lederlønnssamtale én gang i året, som regel i løpet av våren. Lederlønnssamtalen tar utgangspunkt i lederlønnskontrakten. Gjennom lederlønnssamtalen vil departementet vurdere direktørens resultatoppnåelse, og direktøren gir en egenvurdering. I samtalen settes nye mål og resultatkrav for direktøren for det kommende året. Lederlønnskontrakten revideres i forbindelse med lederlønnssamtalene.

### **3.2.4 Rapportering gjennom året**

Datatilsynet skal ha samlet oversikt over bevilgninger de forvalter. De skal levere en regnskapsrapport med status pr. 31. august, med estimert forbruk ut året, sortert på kapittel og post. Det skal rapporteres både på utgifts- og inntektskapittel, og belastningsfullmakter. Vesentlige avvik i forhold til budsjettammer og forutsetninger skal forklares.

Virksomheten skal etterleve de rapporteringskrav som følger av rundskriv for rapportering knyttet til statsbudsjettet og statsregnskapet, herunder eventuelle bestillinger fra departementet.

Virksomheten skal i løpet av året redegjøre for risikovurderinger og eventuelle risikoreduserende tiltak knyttet til vesentlige risikoer, jf. punkt 4.2.1.

Krav til øvrig rapportering og kontroll vurderes av departementet, og vil bli tilpasset de styringsbehov departementet til enhver tid har. Så langt det er mulig vil denne type krav fremgå av de årlige tildelingsbrev.

### **3.2.5 Oppfølging av saker fra Riksrevisjonen**

Departementet skal ha kopi av all korrespondanse mellom virksomheten og Riksrevisjonen. Datatilsynet skal rapportere i det årlige etatsstyringsmøtet og i årsrapporten om hvordan eventuelle merknader fra Riksrevisjonen er fulgt opp, herunder hvilke tiltak som er iverksatt og effekten av disse.

### **3.2.6 Årsrapport**

Årsrapporten fra Datatilsynet utarbeides i overensstemmelse med de krav som stilles i personvernforordningen artikkel 59, i årlige tildelingsbrev og i denne instruks. Årsrapporten skal gi et dekkende bilde av virksomhetens resultater, og gi departementet grunnlag for å vurdere måloppnåelse og ressursbruk.

Virksomheten skal sende årsrapporten elektronisk til departementet innen den fristen som fremgår av tildelingsbrevet. Årsrapporten behandles i etatsstyringsmøtet. Datatilsynet skal offentliggjøre årsrapporten sammen med revisjonsberetningen på sine nettsider så snart etatsstyringsmøtet er avholdt, og senest 1. mai. Dersom revisjonsberetningen ikke er mottatt innen denne frist, skal beretningen publiseres så snart den foreligger.

Årsrapporten skal ha følgende titler og rekkefølge, og utarbeides i samsvar med nærmere krav i Veiledningsnotat til årsrapport for statlige virksomheter:

I Leders beretning

- lederens overordnede vurdering av de samlede resultater, måloppnåelse og ressursbruk og for året i lys av tilstand og utvikling pr hovedmål
- overordnet framstilling av de viktigste prioriteringene for året
- kort omtale av de sentrale forhold, interne og eksterne, som har hatt betydelig innvirkning på oppnådde resultater
- direktørens signatur og dato

II Introduksjon til virksomheten og hovedtall

- kort omtale av virksomheten og samfunnsoppdraget
- kort omtale av organisasjon og ledelse
- presentasjon av utvalgte hovedtall, herunder:
  - antall ansatte og årsverk for de tre siste år<sup>1</sup>
  - samlet tildeling på post 01-99
  - utnyttelsesgrad av post 01-29
  - driftsutgifter
  - lønnsandel av driftsutgifter
  - lønnsutgifter per årsverk
  - antall saker
  - antall vedtak
  - antall påklagede vedtak (ekskl. offentlighetsloven)
  - antall omgjøringer, jf. forvaltningsloven § 33 andre ledd
  - antall oversendelser til Personvernemnda

III Årets aktiviteter og resultater

- overordnet rapportering om aktiviteter og resultater basert på oppgaver som følger av personvernforordningen artikkel 57 nr. 1
- redegjørelse for arbeid med utvalgte hovedprioriteringer
  - gjennomførte aktiviteter
  - overordnet om ressursbruk per hovedprioritering
  - måloppnåelse per hovedprioritering
- en samlet vurdering av prioriteringer, ressursbruk, resultater og måloppnåelse; omtalen skal redegjøre for hvordan Datatilsynets valg av aktiviteter og bruk av ressurser har bidratt til å nå hovedmålet
- en liste over hvilke typer overtredelser som er meldt og hvilke type tiltak som er truffet i samsvar med personvernforordningen artikkel 58 nr. 2

I tillegg skal virksomheten omtale vesentlige forhold i løpet av året som har betydning for departementets styring og oppfølging under de punktene der dette er relevant.

---

<sup>1</sup> Det skal oppgis tall for både antall ansatte og antall avtalte årsverk som hentes fra SSBs statistikk. I tillegg skal det oppgis antall utførte årsverk tilgjengeliggjøres fra DFØ som egen rapport i lønnsystemet for sine lønnskunder. DFØ-tallet skal også tas inn i noteinformasjon i årsregnskapet.

#### IV Styring og kontroll i virksomheten

- virksomhetens overordnede vurdering av opplegget for styring og kontroll
- redegjørelse for vesentlige forhold eller endringer ved virksomhetens planlegging, gjennomføring og oppfølging, herunder:
  - virksomhetens risikostyring
  - status internkontroll, herunder dokumentasjon og iverksatte tiltak
  - bemannings-, kapasitets- og kompetansesituasjonen i virksomheten
  - prosjekter og igangsatte tiltak knyttet til virksomhetens systemer
  - forvaltningen av egne eiendeler (materielle verdier), innkjøpsrutiner mv.
  - oppfølging av ev. avdekkede vesentlig styringssvikt/feil/mangler/utfordringer, herunder merknader fra Riksrevisjonen
  - oppfølging av evalueringer, rapporter fra tilsyn gjennomført hos Datatilsynet og eventuelle pålegg fra tilsynsmyndigheter
- rapportering på vesentlige forhold knyttet til personalmessige forhold, likestilling og diskriminering, bruk av lærlinger, HMS/arbeidsmiljø, ytre miljø og lignende
- redegjørelse for arbeidet med fellesføringer fra regjeringen og eventuelle andre rapporteringskrav som fremgår av tildelingsbrev og denne instruksen

#### V Vurdering av framtidsutsikter

- overordnet omtale av forhold i og utenfor virksomheten som kan påvirke virksomhetens evne til å løse samfunnsoppdraget på sikt og omtale av mulige konsekvenser for virksomhetens evne til å nå fastsatte mål og resultater på lengre sikt

#### VI Årsregnskap

- årsregnskapet skal inneholde følgende tre deler:
  - ledelseskomentarer med virksomhetsleders signatur
  - oppstilling av bevilgningsrapportering med noter
  - oppstilling av artskontorrapportering med noter

### 3.3 Kommunikasjon, ansvar for avklaringer og informasjonsplikt mellom departement og virksomhet

Dersom det er uklårheter i de rammer, målsetninger og føringer som formidles, skal Datatilsynet ta dette opp med departementet. Datatilsynet skal også informere departementet snarlig dersom det oppstår vesentlige avvik med betydning for virksomheten, herunder evnen til å utføre oppgaver i samsvar med personvernforordningen art. 57 og tildelt budsjett.

Dersom Datatilsynet ser at gjeldende regelverk kan ha/har vesentlige utilsiktede konsekvenser, skal virksomheten informere departementet om dette. Datatilsynet skal også uoppfordret gi departementet beskjed dersom virksomheten ser mulige forbedringstiltak som departementet kan iverksette (endringer i lov, forskrift, instruks), som kan bidra til å nå overordnede målsetninger i personvernarbeidet. Departementet vil også kunne be om særskilte evalueringer i forbindelse med regelverksendringer.

Virksomheten skal orientere departementet før offentliggjøring av viktige saker, utredninger, evalueringer eller rapporter som virksomheten har utført eller bestilt, og som det er viktig at departementet kjenner til.

Datatilsynet skal ha en aktiv holdning til kommunikasjon, både internt og eksternt. Det er viktig at Datatilsynet fanger opp signaler i samfunnet som angår Datatilsynet og bruker dette i kommunikasjonsarbeidet. Departementet forventer at Datatilsynet synliggjør sine resultater

innenfor sitt politikkområde og har kontakt med departementet om saker som politisk ledelse kan være med å synliggjøre.

Datatilsynet skal også følge opp klarspråkarbeidet og arbeide systematisk for at dokumenter, brev, nettsider og skjema er brukertilpasset og har klart språk (veiledning og tips finnes på nettsiden klarspråk.no).

### **3.4 Administrative fullmakter**

Departementet gir Datatilsynet følgende administrative fullmakter:

#### **3.4.1 Ansettelser, opprettelse av stillinger og lønnsfastsettelse**

Fullmakten gjelder adgang til å ansette, opprette nye stillinger og fastsette lønn, i den grad ikke annet er bestemt ved lov eller framgår av unntakene nedenfor.

1. Departementet har ansvar for ansettelse av direktør i Datatilsynet.
2. Departementet saksbehandler og avgjør også saker om direktørens arbeidsforhold, for eksempel:
  - alle typer permisjoner (utdanningspermisjon, velferdspermisjon mv.)
  - alle typer lønnsjusteringer (både midlertidige og permanente)

#### **3.4.2 Erstatningskrav mot staten**

Fullmakten gjelder behandling av saker om erstatningskrav mot staten, der utbetalingen ikke overstiger kr 200 000. Med statens erstatningsansvar menes her erstatning på grunnlag av alminnelige erstatningsregler, med unntak av ansvar i kontraktsforhold og ansvar i forbindelse med statens forretningsdrift. Saker skal behandles i tråd med retningslinjene i Justisdepartementets rundskriv G-01/2017, hvor det blant annet forutsettes at det foretas en juridisk vurdering av sakens erstatningsrettslige side før avgjørelsen treffes.

#### **3.4.3 Administrative bestemmelser om flytting til/fra utlandet**

Fullmakten gjelder beslutninger om dekning av utgifter som påløper i forbindelse med flytting fra utlandet i samsvar med retningslinjene i Statens personalhåndbok pkt. 10.6.4 del 2 om Flytting fra utlandet.

#### **3.4.4 Utdanningspermisjon ved studiereiser til utlandet**

Fullmakten gjelder innvilgelse av utdanningspermisjon med lønn i inntil ett år til studiereiser til utlandet, jf. Statens personalhåndbok pkt. 10.8.3.2.

#### **3.4.5 Arbeidsgiverfinansierte elektroniske kommunikasjonstjenester**

Fullmakten gjelder beslutninger om hvem i virksomheten som tilstås arbeidsgiverfinansierte elektroniske kommunikasjonstjenester dekket innenfor virksomhetens eget budsjett. Tildeling av elektroniske kommunikasjonstjenester må gis i samsvar med retningslinjene i Statens personalhåndbok, pkt. 10.2 elektroniske kommunikasjonstjenester (telefon mv.).

## **4. DATATILSYNETS INTERNE STYRING**

### **4.1 Virksomhetsledelsens myndighet og ansvar**

Direktøren er Datatilsynets øverste leder. Direktøren leder Datatilsynet innenfor gjeldende lover, forskrifter, reglementer, retningslinjer, instruksjer og budsjetter.



Direktøren skal fastsette instruks for virksomhetens interne økonomi- og virksomhetsstyring innenfor rammen av denne instruks.

#### **4.1.1 Godtgjørelser/andre utbetalinger til direktøren**

Det skal foreligge rutiner for kontroll og godkjennelse av utleggsrefusjoner og oppgavepliktige tilleggssytelser til direktøren.

## **4.2 Virksomhetens interne styring**

Datatilsynet skal utarbeide strategi for virksomheten, samt interne styringsdokumenter i form av virksomhetsplan, årsplan eller tilsvarende. Det skal også utarbeides budsjett og prognoser for å sikre avviksrapporing og mulighet for oppfølging av regnskap, resultater og måloppnåelse.

Strategier og interne styringsdokumenter skal ha både ettårig og flerårig perspektiv.

Virksomheten skal i sin interne styringsprosess sørge for å utnytte tildelte ressurser effektivt og se på mulighet for å øke produktiviteten. Digitalisering av arbeidsprosesser og tjenester (digitalt førstevalg) er et sentralt virkemiddel, sammen med f.eks. omorganisering, prosessforbedring og annen bruk av teknologi. Det vises til det til enhver tid gjeldende digitaliseringsrundskriv med krav og pålegg om digitalisering i offentlig sektor.

Virksomhetens systemer og rutiner skal sikre etterfølgelse av regelverket for offentlige anskaffelser. Virksomhetens strategi for innkjøp, og oppfølging av denne, skal bidra til at det foretas gode anskaffelser mest mulig effektivt, samt fremme innovasjon og nytenkning i anskaffelsesprosessen. Innkjøpsarbeidet bør inngå i ledelsens internkontroll, slik at uheldig praksis kan korrigeres så snart som mulig. Virksomheten skal med jevne mellomrom evaluere sin innkjøpspraksis.

Virksomheten skal følge etiske retningslinjer i staten og videreutvikle den etiske bevisstheten blant de ansatte.

### **4.2.1 Risikostyring**

Risikostyring skal skje innenfor et samlet rammeverk for styring og kontroll. Datatilsynet skal bruke risikostyring som verktøy i sin mål- og resultatstyring. God risikostyring skal også gi bedre utnyttelse av de midler som er stilt til disposisjon. Risikovurderingene skal relateres til de mål Datatilsynet har satt for sin virksomhet og inngår således som en integrert del av den interne styringen. Der hvor det vurderes å være høy risiko skal risikoreducerende tiltak iverksettes. Det skal gjøres vurderinger av gjenværende risiko, og om denne er akseptabel.

Datatilsynets overordnede risikovurderinger for året oversendes departementet sammen med årsrapport for foregående år, og tas opp som fast tema på etatsstyringsmøtet.

### **4.2.2 Evalueringer**

Det vises til krav i Reglement for økonomistyring i staten § 16 om evalueringer av virksomhetens oppgaveløsning og virkemiddelbruk.

Datatilsynet skal bruke evalueringer systematisk som del av virksomhetsstyringen. Datatilsynet skal sørge for at det gjennomføres evalueringer for å få informasjon om effektivitet, måloppnåelse og resultater innenfor hele eller deler av virksomhetens ansvarsområde og aktiviteter. Frekvens og omfang av evalueringene skal bestemmes ut fra risiko og vesentlighet samt kvalitet og omfang av Datatilsynets øvrige rapportering. Departementet vil kunne be Datatilsynet gjennomføre evalueringer i forbindelse med praksis- og regelverksendringer.

Resultatinformasjonen fra gjennomførte evalueringer skal benyttes i virksomhetens planlegging for de påfølgende årene.

Evalueringer som er gjort tilgjengelig for allmenheten, skal registreres i Evalueringsportalen.

#### **4.2.3 Arbeidsgiverrollen (HMS og likestilling)**

Datatilsynet skal følge opp statlig arbeidsgiverpolitikk, herunder implementere føringer og følge opp rapporteringer på personalområdet.

Datatilsynet skal ha et system for å kartlegge og følge opp risiko- og problemområder innen helse, miljø og sikkerhet, jf. Lov av 17. juni 2005 nr 62: Lov om arbeidsmiljø, arbeidstid og stillingsvern mv.

Videre skal Datatilsynet arbeide målrettet og planmessig for å fremme likestilling og hindre diskriminering på grunn av kjønn, graviditet, permisjon ved fødsel og adopsjon, omsorgsoppgaver, etnisitet, religion, livssyn, funksjonsnedsettelse, seksuell orientering, kjønnsidentitet og kjønnsuttrykk. Dette fremgår av § 26 i likestillings- og diskrimineringsloven. Virksomheten har en aktivitets- og redegjøringsplikt og arbeidet skal skje fortløpende og i samarbeid med de ansattes representanter.

Datatilsynet skal avgi en likestillingsredegjørelse for foregående år. Rapporteringen skal følge gjeldende veiledning på området.

Datatilsynet skal, alene eller i samarbeid med andre virksomheter, knytte til seg minst én lærling i sin virksomhet og hvert år vurdere om det er mulig å øke antall lærlinger og tilby opplæring i nye lærefag. For å styrke en felles innsats for å rekruttere lærlinger og bidra til et yrkesfaglig løft, skal virksomheten knytte seg til opplæringskontoret OK stat eller et annet opplæringskontor.

Det skal rapporteres om bruk av lærlinger i årsrapportens del IV.

#### **4.2.4 Regnskapsprinsipp og regnskapsføring**

Datatilsynet skal utarbeide et virksomhetsregnskap i samsvar med kontantprinsippet, bruttoprinsippet, ettårsprinsippet og fullstendighetsprinsippet, jf. Bestemmelsene pkt. 3.4.2, og i tråd med årlige og varige rundskriv fra Finansdepartementet.

Datatilsynet avgjør i samråd med departementet eventuelle endringer i regnskapsprinsipp for virksomhetsregnskapet, jf. Bestemmelsene pkt. 3.4.2.

Virksomheten skal bruke standard kontoplan som føringskontoplan, og skal rapportere til statsregnskapet etter statens kontoplan.

### **4.3 Krav til virksomhetens internkontroll**

Datatilsynets ledelse har ansvar for å innrette virksomhetens systemer og rutiner for internkontroll, og påse at nødvendige kontrolloppgaver blir utført. Risiko- og vesentlighetsvurderinger skal ligge til grunn. Datatilsynet skal rapportere umiddelbart til departementet dersom det avdekkes vesentlige svakheter, feil eller mangler i kritiske prosesser eller aktiviteter i virksomheten.

Risikovurdering og styring på bakgrunn av dette skal skje innenfor et samlet rammeverk for styring og kontroll, se punkt 4.2.1.

### **4.4 Virksomhetens arbeid med sikkerhet**

#### **4.4.1 Samfunnssikkerhet og beredskap**

Det legges til grunn at arbeid med samfunnssikkerhet og beredskap inngår som en integrert del av all virksomhet i Datatilsynet. Departementet forventer at Datatilsynet foretar skriftlig kartlegging av risiko og sårbarhet på eget ansvarsområde, at det utarbeides nødvendige beredskaps- og kriseplaner, og anbefaler at Datatilsynet hvert år arrangerer eller deltar i krise- og beredskapsøvelser.

Virksomheten skal årlig utarbeide en kortfattet, overordnet og sammenstilt risiko- og sårbarhetsvurdering for virksomheten (ROS-vurdering).

Datatilsynet skal sende en rapport som inneholder den overordnede ROS-vurderingen, en omtale av virksomhetens kompetanse på området og plan for nødvendig kompetanseheving innen samme frist som årsrapporten.

Lov om forebyggende sikkerhetstjeneste (sikkerhetsloven) med tilhørende forskrifter gjelder for alle forvaltningsorganer som er i besittelse av skjermverdig informasjon eller objekt. Datatilsynet skal innen samme frist som for årsrapporten, sende en egen rapport om sikkerhetstilstanden til departementet.

Rapporten skal særskilt redegjøre for oppfølging av eventuelle mangler og avvik som Datatilsynet har identifisert siden forrige rapportering. Datatilsynet må vurdere nivå på sikkerhetsgradering av rapport om sikkerhetstilstand som sendes KMD. Datatilsynet skal vurdere behov for å sikkerhetsklarere personell, jf. sikkerhetsloven med tilhørende forskrifter. Datatilsynets direktør skal være sikkerhetsklarert og autorisert av departementet. Ansatte med tjenstlig behov skal også være sikkerhetsklarert og autorisert.

#### **4.4.2 Informasjonssikkerhet**

Datatilsynet skal beskrive mål og strategi for informasjonssikkerhet i virksomheten (sikkerhetsmål og sikkerhetsstrategi). Disse skal danne grunnlaget for Datatilsynets internkontroll (styring og kontroll) på informasjonssikkerhetsområdet. Sikkerhetsstrategien og internkontrollen skal inkludere relevante krav som er fastsatt i annen lov, forskrift eller instruks.

Datatilsynet skal ha en internkontroll (styring og kontroll) på informasjonssikkerhetsområdet som baserer seg på anerkjente standarder (f.eks. ISO27001/27002) for styringssystem for informasjonssikkerhet.

Internkontrollen bør være en integrert del av Datatilsynets helhetlige styringssystem. IKT-systemer og informasjonsaktiva skal klassifiseres og risikovurderes for å sikre hensynet til informasjonens konfidensialitet, integritet og tilgjengelighet. Klassifisering og risikovurdering er særlig viktig i forbindelse med anskaffelser av IKT-utstyr og -systemer. Omfang og innretning på internkontrollen skal være tilpasset risiko.

Hendelser som truer eller kompromitterer informasjonssikkerheten skal rapporteres.

Informasjonssikkerhet vil være et tema i styringsdialogen. En overordnet statusrapport for arbeidet skal fremkomme av årsrapporten.