FINANSMINISTERIET

Vejledning om tilsynet med Økonomi-styrelsens fælles-statslige systemer

2019

Indhold

1. Indledning

Formålet med vejledningen er at beskrive Finansministeriets departements tilsyn med Økonomistyrelsen. Tilsynet er baseret på det fællesstatslige tilsynskoncept, som er obligatorisk og beskriver departementets overordnede tilsynsansvar.

Baggrunden er, at det fremgår af regnskabsbekendtgørelsen, at alle stats- og selvejende institutioner skal anvende de systemer på økonomi-, betalings- og HR- og lønområdet (§11 stk. 1 og 2), der stilles til rådighed af Økonomistyrelsen. Det fremgår ligeledes af regnskabsbekendtgørelsen, at Økonomistyrelsen har ansvaret for at stille de relevante krav til systemernes drift og sikkerhed, herunder vedrørende persondata, og for at sikre overholdelse af kravene (§6 stk. 5).

Med ISO 27001-standarden, samt med hjælp af et ISMS-værktøj, har Økonomistyrelsen en struktureret tilgang til informationssikkerhed og risikostyring. På baggrund heraf har Økonomistyrelsen etableret et ledelsessystem med de kontroller, der er nødvendige for at håndtere de specifikke risici.

Økonomistyrelsen har i samarbejde med Datatilsynet udarbejdet en cirkulæreskrivelse om fælles dataansvar vedrørende Økonomistyrelsens fællesoffentlige systemer. Efter artikel 26 i GDPR foreligger der fælles dataansvar, når to eller flere dataansvarlige i fællesskab fastlægger formålene med og hjælpemidlerne til behandling af persondata. Dette er tilfældet for de fællesoffentlige systemer på økonomi-, betalings-, HR- og lønområdet, som Økonomistyrelsen leverer iht. regnskabsbekendtgørelsen.

På Økonomistyrelsens hjemmeside er der – bl.a. i form af en række servicebeskrivelser – oprettet oplysninger om, hvilke fælles systemer i staten Økonomistyrelsen leverer, hvilke processer disse systemer understøtter, samt hvilke data der findes i systemerne.

Kontor for Revision og Tilsyn (KRT) i Finansministeriets departement varetager tilsynet med Økonomistyrelsens fællesstatslige systemer (kaldt fremover i tilsynsrapporten).

Vejledningen er godkendt af Økonomistyrelsens ledelse og Finansministeriets Departement.

2. Formål og omfang

Formålet med tilsynet er at vurdere, om informationssikkerhed og GDPR (EU's databeskyttelsesforordning) i Økonomistyrelsen er tilrettelagt hensigtsmæssigt, pålideligt og sikkerhedsmæssigt forsvarligt, så informationers fortrolighed, integritet og tilgængelighed sikres i overensstemmelse med det regelgrundlag, styrelsen er underlagt.

Indholdet af tilsynet med informations- og datasikkerhed omfatter eksempelvis de forpligtelser, der påhviler Økonomistyrelsen i forhold til styring af informationssikkerhed efter ISO 27001, efterlevelse af databeskyttelsesloven og -forordningen og opfølgning på bemærkninger fra revisions- og tilsynsmyndigheder.

Den nærmere proces og rapportering er beskrevet i KRT's notat om FM's proces for det departementale tilsyn med informations- og datasikkerhed i FM. Overordnet indeholder tilsynet en vurdering og test af, om relevant lovgivning og standard på sikkerhedsområdet er overholdt og implementeret i relevante processer, procedurer, kontroller osv. I de efterfølgende afsnit er relevante afsnit, formuleringer, tabeller mm. fra KRT's notat gengivet.

Det enkelte tilsyn har til formål at konkludere og rapportere til ledelsen på de 6 fokusområder i tabel 1. Udkast til en tilsynsrapport forelægges for Økonomistyrelsens daglige ledelse og endelig tilsynsrapport for styrelsens topledelse.

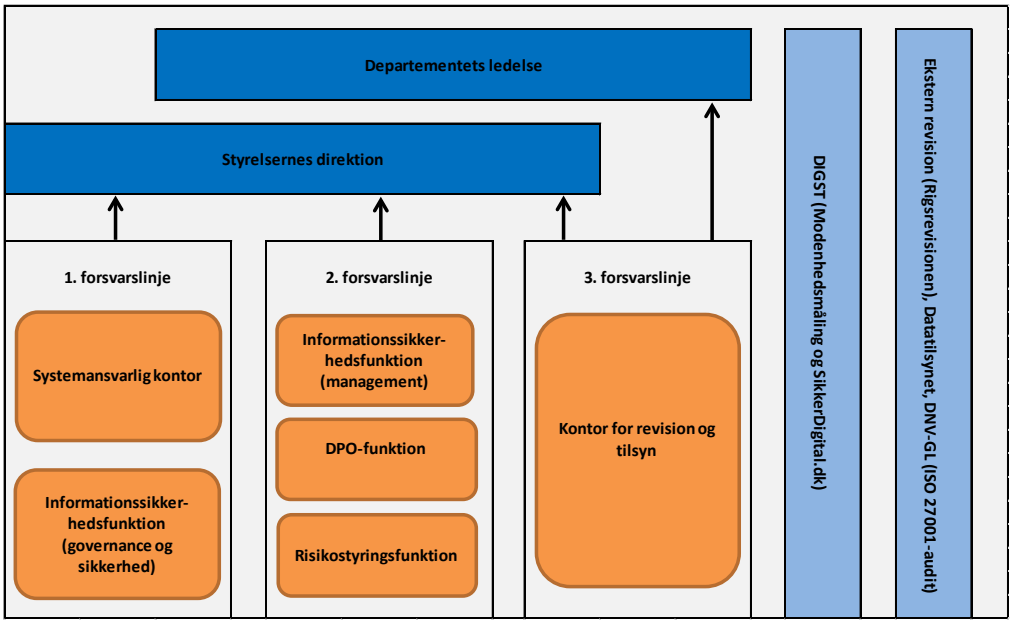
Tabel 1
Vurdering af modenhed og effektivitet (jf. bilag 1)

Fokusområder	Compliance (modenhed)	Vurdering og test (effektivitet)
• Institutionens ledelse har **tilrettelagt en styring**, der sikrer, at informationssikkerheden er fastlagt og håndteret hensigtsmæssigt		
• Institutionens **generelle it-kontroller** sikrer et, efter institutionens forhold, betryggende sikkerhedsniveau		
• Institutionen periodisk foretager en **risikovurdering** af informationssikkerheden for at identificere risiko for tab af fortrolighed, integritet og tilgængelighed		
• Institutionen har fastlagt **politikker og retningslinjer** for informationssikkerheden		
• Institutionen har etableret **procedurer og kontroller**, som sikrer en betryggende databeskyttelse og behandling af personoplysninger		
• Institutionen har taget stilling til **bemærkninger og anbefalinger fra revisions- og tilsynsmyndigheder**		

3. Organisering og delegering af ansvar

Gennem en governance model vises fordelingen af roller og ansvar på tværs af de tre forsvarslinjer. Modellen beskriver tilsynets rolle i Økonomistyrelsens governance struktur, dvs. at det udførte tilsyn vil dække de kontrolaktiviteter, der udføres i både første og anden forsvarslinje.

Figur 1 De tre forsvarslinjer



Præcisering og uddybning af de indsatte funktioner:

- *Systemansvarligt kontor* består af systemkontorer i Center for Systemer samt Statsregnskabskontoret. Ejer og håndterer risici og tilhørende kontrolaktiviteter.
- *Informationssikkerhedsfunktionen* består i første forsvarslinje af en enhed som er forankret i Systemcentret. Monitorerer håndteringen af risici og kontrolaktiviteter på vegne af ledelsen. Anden forsvarslinje skal støtte ledelsen gennem deres særlige ekspertise og procesindsigt på tværs af organisationen, således at de (sammen med første forsvarslinje) medvirker til at sikre, at risici og kontroller håndteres og styres effektivt.
- *Risikostyring* i Finansministeriet sker ved, at direktionerne risikovurderer projekter/opgaver iht. et fælles risikostyringskoncept. KRT koordinerer og indsamler vurderingerne. Risikostyringsoversigten forelægges og drøftes i Driftsledelsen kvartalsvist.
- *Kontor for revision og tilsyn* påser compliance niveauet og effektiviteten i håndteringen af risici og kontroller til brug for den øverste ledelse. Herudover

er kontoret uafhængige af ledelsen, hvilket er med til at sikre objektivitet i det udførte tilsynsarbejde.

4. Intern audit (tilsyn og revision)

Tilsynet har en væsentligheds og risikobaseret tilgang til hvilke emner, der indgår i tilsynsplanen. Dog vil tilsynet som minimum dække de områder, som kunder i Økonomistyrelsen har en vis interesse i.

KRT anvender en referenceramme, som efter vores opfattelse dækker alle væsentlige aktiviteter. Her i vejledningen er uddrag i form af anvendte tabeller gengivet. De understøtter tilsynet og afdækker efterlevelse af kravene i ISO-standarden og relevante GDPR-regler.

4.1 Styring af informationssikkerhed

Nedenfor er tabel 2 gengivet. Den sammenfatter den obligatoriske dokumentation i et ledelsessystem for informationssikkerhed og viser herigennem, om Økonomistyrelsen er tilstrækkelig compliant og fastholder det nødvendige complianceniveau (ISO-reference K.9.2).

Tabel 2
ISMS (Information Security Management System)

ISO-ref.	Krav i ISO 27001	Compliance af ØS[1]	Vurdering og test af KRT
K.4	Organisationens kontekst (omfanget af ISMS)		
K.5	Lederskab (ledelsesforankring og organisering)		
K.6	Planlægning (rammer for it-risikostyring)		
K.7	Support (uddannelse og awareness)		
K.8	Drift (risikovurdering, risikohåndtering og ajourf. SoA)		
K.9	Evaluering (overvågning, måling, analyse og evaluering)		
K.10	Forbedring (afvigelser og korrigerende handlinger)		

Compliance = Påvise/dokumentere efterlevelse af ISO-krav vedr. procedurer og processer.
Vurdering og test = Afprøve udvalgte procedurer og processer.
"Trafiklys" = Anvende grøn, gul og rød, hvor grøn indikerer overensstemmelse med ISO-standardens krav, gul indikerer mangler og rød indikererer væsentlige mangler.

[1] Økonomistyrelsens selvevaluering. Den dækker områderne indenfor ISMS i ISO 27001.

4.2 Implementering af generelle it-kontroller

Nedenfor er tabel 3 gengivet. Den sammenfatter Økonomistyrelsens selvevaluering af, at der for de påtagne risici er implementeret de nødvendige kontroller, og at disse er effektive. KRT udfører et antal af test af kontroller for at vurderere styrelsens egenvurdering eller senest opdaterede SoA-dokument med til- og fravalg af kontroller (ISO-reference A.18.2.1).

Tabel 3
Generelle it-kontroller

ISO-ref.	Sikkerhedskontroller i ISO 27001	Best practice m.m. af ØS	Vurdering og test af KRT
A.5	Informationssikkerhedspolitikker		
A.6	Organisering af informationsikkerhed		
A.7	Personalesikkerhed		
A.8	Styring af aktiver		
A.9	Adgangsstyring		
A.10	Kryptografi		
A.11	Fysisk sikring og miljøsikring		
A.12	Driftssikkerhed		
A.13	Kommunikationssikkerhed		
A.14	Anskaffelse, udvikling og vedligeholdelse af systemer		
A.15	Leverandørforhold		
A.16	Styring af informationssikkerhedsbrud		
A.17	Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring		
A.18	Overensstemmelse		

Best practice m.m. = Beskrive, hvordan Økonomistyrelsen gennemfører kontroller.
Vurdering og test = Afprøve de implementerede kontroller.
"Trafiklys" = Anvende grøn, gul og rød, hvor grøn indikerer fuldt implementeret, gul delvist implementeret og rød indikerer ikke implementeret.

4.3 Implementering af GDPR

Nedenfor er tabel 4 gengivet. Den viser skemaet i 2019 version til Økonomistyrelsens selvevaluering af de kontrolaktiviteter, som styrelsen har designet, implementeret og udført for at sikre sig efterlevelse af krav i det fælles dataansvar. KRT udfører et antal af test af kontroller for at vurdere relevansen og effektiviteten.

Tabel 4
Økonomistyrelsen med fælles dataansvar

CIS[2]	Artikel i GDPR	Kontrolmål	Compliance af ØS	Vurdering og test af KRT
3.3	5 – Principper for behandling af personoplysninger	Der efterleves procedurer og kontroller, som sikrer, at indsamling, behandling og opbevaring af personoplysninger sker i overensstemmelse med principperne for behandling af personoplysninger		
3.1 3.2	6 – Lovlig behandling	Der efterleves procedurer og kontroller, som sikrer, at der alene sker lovlig behandling af personoplysninger.		
4.3 4.4	12 - Gennemsigtig oplysning, meddelelser og nærmere regler for udøvelsen af den registreredes rettigheder	Der efterleves procedurer og kontroller, som sikrer, at udøvelsen af den registreredes rettigheder sker rettidigt, herunder besvarelse af den registreredes anmodninger og begrundelse af eventuelt afslag.		
5.2	24 – Implementering af passende databeskyttelse	Der efterleves procedurer og kontroller, som sikrer, at databehandlerens tekniske og organsatoriske foranstaltninger til beskyttelse af den registrerede rettigheder og behandlingen af personoplysninger er godkendt af den dataansvarlige.		
5.3	25 – Databeskyttelse gennem design og standardindstillinger	Der efterleves procedurer og kontroller, som sikrer, at kravene om databeskyttelse gennem design og standardindstillinger i de tekniske og organisatoriske sikringsforanstaltninger fungerer effektivt.		
6.1 6.2 6.3 6.4	28 og 29 – Behandling af personoplysninger på vegne af den dataansvarlige	Der efterleves procedurer og kontroller, som sikrer, at behandling af personoplysninger alene sker iht. en databehandleraftale samt at databehandlingen alene foretages af databehandlere, som er godkendt af den dataansvarlige.		
7.1 7.2	30 – Fortegnelser over behandlingsaktiviteter	Der efterleves procedurer og kontroller, som sikrer, at den dataansvarlige fører en fortegnelse over kategorier af behandlingsaktiviteter, som foretages i de pågældende systemer.		
8.1	32 – Behandlingssikkerhed	Der efterleves procedurer og kontroller, som sikrer, at der på baggrund af en evaluering af risici er truffet passende tekniske og organisatoriske foranstaltninger mod hændelig eller ulovlig tilintetgørelse, tab, ændring, uatoriseret videregivelse af eller adgang til personlysninger.		

[2] Cirkulæreskrivelse (CIS) nr. 9223 af 23. marts 2018 om fælles dataansvar

Tabel 4
Økonomistyrelsen med fælles dataansvar

9.1 10.1	33 og 34 – Anmeldelse af brud på persondatasikkerheden til tilsynsmyndigheden	Der efterleves procedurer og kontroller, som sikrer, at databehandler ved brud på persondatasikkerheden kan understøtte den dataansvarliges pligt til rettidig og fyldestgørende anmeldelse til tilsynsmyndigheden, samt underretning til de registrerede, hvis personoplysninger er omfattet af bruddet.
11.1 11.2	35 og 36 – Konsekvensanalyse vedr. databeskyttelse og forudgående høring	Der efterleves procedurer og kontroller, som sikrer, at den dataansvarlige forud for behandlingen har en analyse af de påtænkte behandlingsaktiviteteters konsekvenser for beskyttelse af personoplysninger, hvis en type behandling, navnlig ved brug af nye teknologier og i med før af sin karakter, omfang, sammenhæng og formål, sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og fritidsrettigheder. Den dataansvarlige er ligeledes forpligtet til at iagttage kravet i forordningens artikel 36 om forudgående høring af tilsynsmyndigheden, når kravet findes anvendelse.
12.1	44, 45 46, 47, 48, 49 og 50 – Overførsel af personoplysninger	Der efterleves procedurer og kontroller, som sikrer, at der alene sker overførsel af personoplysninger til et tredjeland eller en internatio-nal organsiation, hvis Kommisionenen har fastslået, at tredjelandet, et område eller en eller flere specifikke sektorer i dette tredjeland, eller den pågældende internationale organisation har et tilstrækkeligt beskyttelsesniveau.

Compliance = Påvise/dokumentere efterlevelse af GDPR-krav ved procedurer og kontroller.
Vurdering og test = Afprøve udvalgte procedurer og kontroller.
"Trafiklys" = Anvende grøn, gul og rød, hvor grøn indikerer overensstemmelse med kravene i GDPR, gul mangler og rød væsentlige mangler.

4.4 Status og fremdrift på bemærkninger

KRT registrerer alle opstartede og afsluttede revisioner/undersøgelser i Økonomistyrelsen i en FM RevisionsDatabase (FRD). De pågældende enheder udarbejder handlingsplaner og gennemførelsesfrister for evt. afgivne observationer og risici (bemærkninger) i FRD. En revisionskoordinator i Økonomistyrelsen varetager styrelsens interesser i relation til håndtering af revisioner/undersøgelser og den løbende opfølgning.

Med udgangspunkt i de registrerede data i FRD udarbejder KRT en oversigt over revisioner/undersøgelser i indeværende år og vurderer om der er fremdrift i håndtering af de væsentligste risici på de reviderede/undersøgte områder.

5. Rapportering fra tilsynet

5.1 Løbende tilsynsrapporteringer

KRT afrapporterer tilsynet med Økonomistyrelsen til ledelsen. Tilsynsrapporten fremsendes i høring inden endelig fremsendelse. I bilag 1 fremgår bedømmelsesskalaen for de løbende tilsynsrapporter.

I de løbende tilsynsrapporter følges endvidere op på udestående bemærkninger fra tidligere år.

5.2 Årlig sammenfatning til Økonomistyrelsens kunder

En gang om året afrapporteres KRT's tilsyn med Økonomistyrelsen til kunderne. Den årlige afrapportering indeholder alene en sammenfatning af eventuelle forhold, som er af væsentlig sikkerhedsmæssig betydning for kunder i forhold til de fællesstatslige systemer. Udkast til tilsynsrapporten med tilhørende sammenfatning til brug for kunderne, drøftes på et møde mellem KRT og Økonomistyrelsen, hvorefter endelig sammenfatning gøres tilgængelig fx sammen med ledelseserklæring fra Økonomistyrelsens ledelse.

6. Henvendelser til tilsynet

Kunder i Økonomistyrelsen kan henvende sig til tilsynet i Finansministeriets departement, såfremt der er risici, som – efter henvendelse til Økonomistyrelsen – ikke løses.
Tilsynet vurderer henvendelsens relevans, karakter og vælger den mest hensigtsmæssige tilsynsbehandling. I rapporteringen af tilsynet med Økonomistyrelsens fællesstatslige systemer vil KRT redegøre for eventuelle henvendelser fra kunder.

Bilag 1 vedrørende kriterier for KRT's bedømmelse i løbende tilsynsrapporter

Rapportens konklusion vil dels indeholde en modenhedsvurdering over en skala med fuldt compliance (pastelgrøn) – ikke helt fuldt compliance (gul) – ikke fuldt compliance (rød). Jo flere krav og relevante procedurer og processer, der efterleves og dokumenteres på en hensigtsmæssigt måde af institutionen, jo højere vurderes modenhed, og dels en graduering. Formålet er, at fremkomme med en vurdering af de implementerede kontroller og sker over en fireskala. Ligeledes oplyses graduering i forhold til en skala betryggende – ikke betryggende. For at sikre en vis ensartethed i vurderingerne er graduering støttet af en matematisk tilgang baseret på antal af observationer fordelt i 3 risikokategorier. Den kan illustreres således:

Meget tilfredsstillende	Betryggende	Ingen eller få observationer med lav risiko
Tilfredsstillende		Enkelte observationer med enten middel eller lav risiko
Ikke helt tilfredsstillende	Ikke betryggende	Enkelte observationer med høj og middel risiko
Ikke tilfredsstillende		Flere observationer med høj og middel risiko

Tilsynets konklusion inkluderer observationer og anbefalinger, som dels fremføres i et bilag til afrapporteringen og dels registreres i FM RevisionsDatabase (FRD). Herved sikres det, at en konklusion ikke blot bliver en passiv tilgang, men at institutionen forholder sig konkret til tilsynets konklusion og dens observationer og deres prioritering.

fm.dk