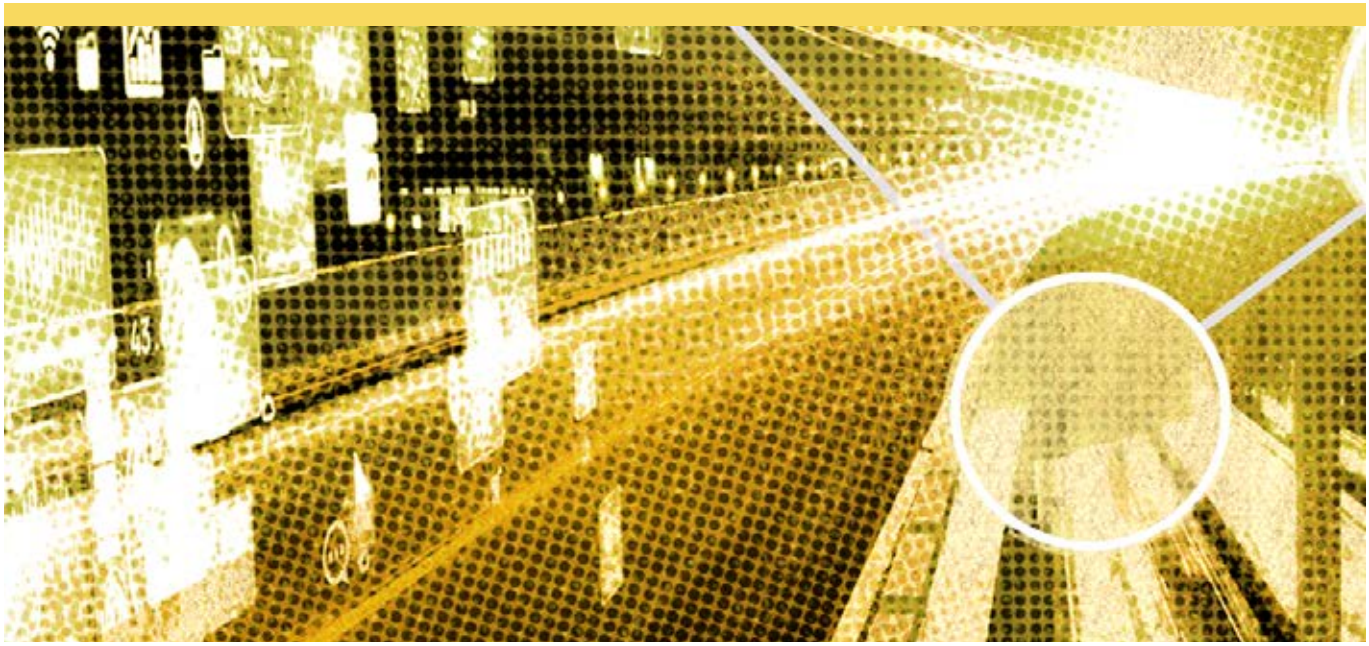
Tilsynet med Efterretningstjenesterne



Årsredegørelse 2021

Center for Cybersikkerhed

Indhold

Til forsvarsministeren

I overensstemmelse med § 24 i lov om Center for Cybersikkerhed (lovbekendtgørelse nr. 836 af 7. august 2019) afgiver Tilsynet med Efterretningstjenesterne hermed redegørelse om sin virksomhed vedrørende Center for Cybersikkerhed for 2021. Redegørelsen skal offentliggøres.

København, maj 2022

Michael Kistrup
Formand for Tilsynet med Efterretningstjenesterne

Resumé

Sigtet med redegørelsen er at give en generel information om karakteren af det tilsyn, der udøves med CFCS.

Tilsynet påser, at CFCS overholder lovens regler om

- indgreb i meddelelseshemmeligheden,
- behandling af personoplysninger i centret,
- analyse, videregivelse og sletning af data og
- krav til sikkerhedsforanstaltninger i forbindelse med centrets behandling af personoplysninger.

Redegørelsen indeholder blandt andet oplysninger om de forhold, som tilsynet har valgt at interessere sig for, og om i hvor mange tilfælde tilsynet har fundet, at CFCS' behandling af personoplysninger ikke har været i overensstemmelse med reglerne.

Tilsynets planlægning af kontroller sker på baggrund af en årlig risiko- og væsentlighedsvurdering af processer og systemer i CFCS. Formålet hermed er at vurdere risici for lovbrud i relation til de af CFCS' aktiviteter, der er omfattet af tilsynets kompetence. Tilsynets kontrol fokuserer på de områder, hvor der er størst risiko for fejl.

For 2021 fremhæves følgende centrale og principielle dele af redegørelsen:

! Tilsynet kan konstatere, at CFCS i **14 tilfælde** ikke overholdt lovgivningens krav til sikkerhedsforanstaltninger i forbindelse med behandling af oplysninger, jf. CFCS-lovens § 18, stk. 1, og centrets interne retningslinjer, men at centrets håndtering af eksterne medier i øvrigt var tilrettelagt i overensstemmelse med lovgivningens krav.

Efter tilsynets vurdering skyldtes 13 af ovennævnte tilfælde, at der i CFCS' interne retningslinjer var uklarhed om, hvorvidt der skulle ske selvstændig registrering af 13 separat opbevarede simkort fra 13 indleverede routere, der i øvrigt var registreret i overensstemmelse med centrets interne retningslinjer. Tilsynet har efterfølgende noteret sig, at CFCS har præciseret de interne retningslinjer med henblik på at imødegå fremtidige fejl. Det sidste tilfælde skyldtes, at et en indleveret telefon manglede en påføring af et sagsnummer og dermed ikke var registreret i overensstemmelse med CFCS' interne retningslinjer (afsnit 1.2.2).

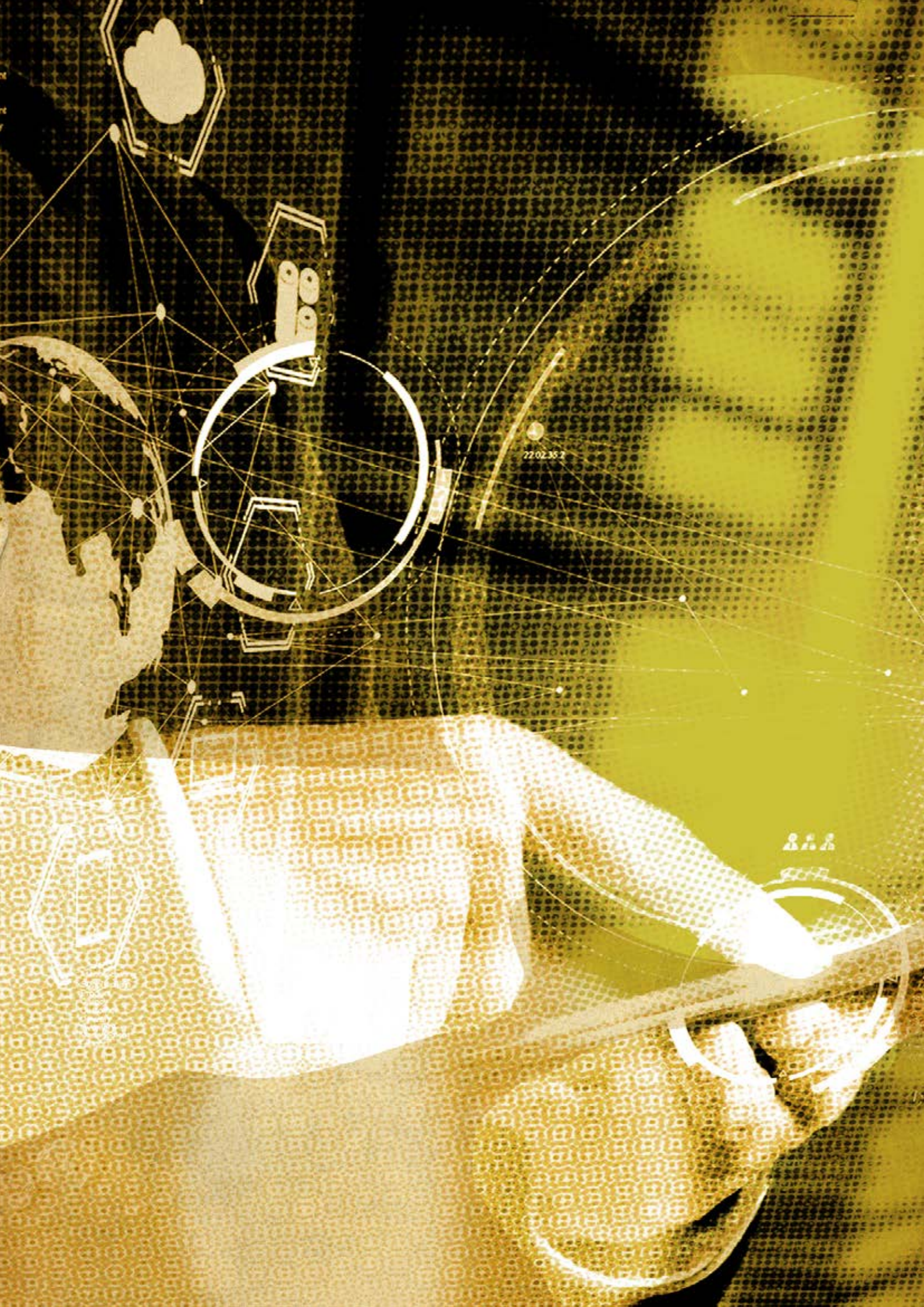
! Tilsynet har **modtaget forsvarsministerens afgørelse** vedrørende CFCS' forpligtelse til at slette data fra centrets sensornetværk i henhold til CFCS-lovens § 17, stk. 1. CFCS indbragte i juli 2020 spørgsmålet om fortolkningen af § 17, stk. 1, for forsvarsministeren, idet centret var uenig i tilsynets fortolkning af forpligtelsen.

Forsvarsministeren vurderer, at sensordata, hvor CFCS efter endt analyse vurderer, at der er tale om en falsk positiv alarm, og som derfor efter centrets opfattelse ikke vedrører en sikkerhedshændelse, ikke skal slettes i henhold til CFCS-lovens § 17, stk. 1, idet formålet med behandlingen ikke er opfyldt.

Forsvarsministeren vurderer endvidere, at CFCS-lovens § 17, stk. 1, i forhold til sensordata har et meget begrænset anvendelsesområde. Bestemmelsens primære anvendelsesområde er derimod de øvrige former for data, der er omfattet af CFCS-lovens kapitel 4.

Forsvarsministerens afgørelse er behandlet nærmere i afsnit 2.

Det bemærkes, at ovenstående henvisninger alene udgør et mindre udsnit af tilsynets kontrol af CFCS i 2021, hvor tilsynet har haft særlige eller principielle bemærkninger. For det fulde billede af tilsynets kontrol af CFCS skal redegørelsen læses i sin helhed.



Skala for tilsynets bemærkninger

Tilsynets bemærkninger tager udgangspunkt i følgende skala:

Bemærkninger	Baggrund for bemærkninger
»[...] **giver ikke anledning til bemærkninger**«	Anvendes når tilsynet er enig med CFCS i, hvordan de generelt eller konkret administrerer loven.
»Tilsynet **finder ikke, at der er grundlag for at kritisere** [...]«	Anvendes når tilsynets prøvelsesmuligheder er begrænset enten af faktiske eller juridiske forhold.
»Tilsynet finder det **bemærkelsesværdigt** [...]«	Anvendes om forhold i CFCS eller lovgivningen, som ikke stemmer overens med det almindelige eller umiddelbare indtryk, som en udenforstående har.
»Tilsynet finder det **problematisk** [...]«	Anvendes om forhold, hvor der ikke er konstateret egentlige lovbrud, men hvor der vurderes at være en stor risiko for, at forholdene kan føre til lovbrud eller hvor tilsynet har været forhindret i et udøve sin virksomhed i en periode af en vis varighed.
»Tilsynet kan **konstatere** [...]«	Anvendes om forhold, hvor der er konstateret egentlige lovbrud af enkeltstående karakter eller brud på interne retningslinjer.
»Tilsynet finder det **kritisabelt** [...]«	Anvendes om forhold, hvor der er konstateret egentlige lovbrud af et ikke uvæsentligt omfang eller hvor tilsynet har været forhindret i at udøve sin virksomhed i en længere periode.
»Tilsynet finder det **overordentligt kritisabelt** [...]«	Anvendes om forhold, hvor der er konstateret alvorlige lovbrud eller hvor tilsynet har været forhindret i at udøve sin virksomhed i en længere periode, uden at CFCS har udvist vilje til sikre den fornødne afhjælpning heraf.

Forord

I 2021 har tilsynets virksomhed været berørt af COVID-19. Tilsynet har været lukket ned fra december 2020 til april 2021, hvilket har påvirket omfanget af tilsynets kontrol af CFCS, idet tilsynets medarbejdere ikke har mulighed for at gennemføre kontrolarbejde hjemmefra.

Tilsynet har til trods for nedlukningen i 2021 gennemført en omfattende og intensiv kontrol af CFCS, hvilket nærværende redegørelse vidner om.

CFCS har til opgave at understøtte et højt informationssikkerhedsniveau i den informations- og kommunikationsteknologiske infrastruktur, som samfundsvigtige funktioner er afhængige af. Denne opgave løses blandt andet ved, at CFCS opdager, analyserer og bidrager til at imødegå avancerede cyberangreb hos Forsvaret samt de statslige myndigheder og virksomheder, der er tilsluttet centrets sensornet.

For at udføre denne samfundsvigtige funktion har CFCS i henhold til lovgivningen meget vide beføjelser til uden retskendelse at foretage indgreb i meddelelseshemmeligheden og efterfølgende behandle oplysninger om borgere og virksomheder. Med henblik på at sikre retssikkerheden for den enkelte borger og virksomhed modsvares CFCS' beføjelser af en række regler for centrets efterfølgende sletning af tilvejebragte oplysninger.

Der påhviler CFCS et stort ansvar at overholde disse regler, da reglerne på samme tid beskytter den enkelte borgers retssikkerhed og sikrer, at centret i kritiske situationer har det nødvendige overblik over alle relevante oplysninger.

Tilsynet har i 2021 modtaget forsvarsministerens afgørelse vedrørende CFCS' forpligtelse til at slette data fra centrets sensornetværk i henhold til CFCS-lovens § 17, stk. 1. CFCS indbragte i juli 2020 spørgsmålet om fortolkningen af § 17, stk. 1, for forsvarsministeren, idet centret var uenig i tilsynets fortolkning af forpligtelsen. Forsvarsministerens afgørelse er behandlet nærmere i redegørelsens afsnit 2.

Efter forsvarsministerens afgørelse finder CFCS-lovens § 17, stk. 1, kun i ganske begrænset omfang anvendelse for sensordata, hvorfor der som det klare udgangspunkt ikke sker en løbende sletning af indhentet sensordata. De absolutte slettefrister i CFCS-lovens § 17, stk. 2, bliver herefter den eneste relevante frist for behandling af indhentet sensordata.

Tilsynet vil fremover lægge forsvarsministerens fortolkning af CFCS-lovens § 17, stk. 1, til grund i forbindelse med kontrollen af CFCS.

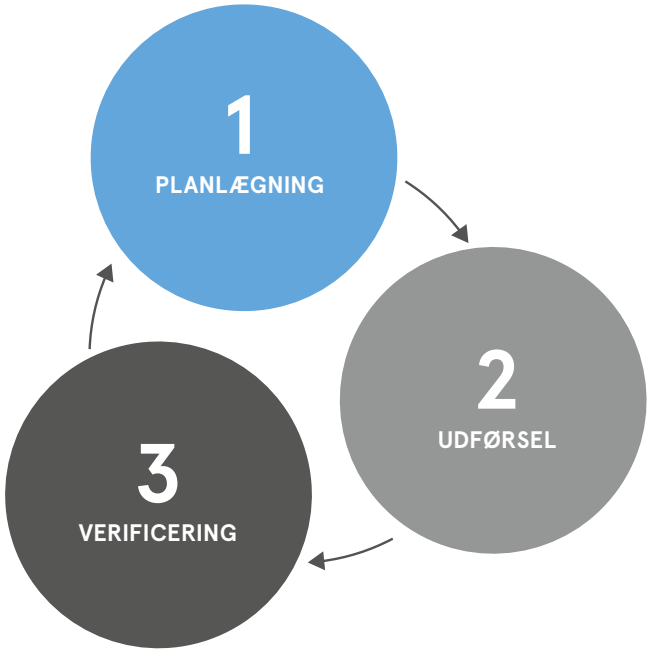
Michael Kistrup
Formand for Tilsynet med Efterretningstjenesterne

1. Tilsynets kontrol

1.1 Kontrolmetode

Tilsynet arbejder kontinuerligt med at forbedre de metoder, som tilsynet anvender i planlægningen og udførelsen af kontrollen af CFCS med henblik på, at kontrollen får den størst mulige effekt inden for de rammer, som er sat for tilsynets virke.

Tilsynets kontrol af CFCS består overordnet af følgende tre delelementer:



Tilsynets **1)** planlægning af kontroller for det kommende år sker på baggrund af en årlig risiko- og væsentlighedsvurdering af processer og systemer i CFCS. Formålet hermed er at vurdere risici for lovbrud i relation til centrets aktiviteter, der er omfattet af tilsynets kompetence. På baggrund heraf udarbejder tilsynet risikoanalyser, som danner grundlag for udvælgelsen af det kommende års kontroller.

Formålet med risikoanalyserne er at sikre, at tilsynets kontrol fokuseres på de områder, hvor der er størst risiko for fejl, samt at der tages højde for andre relevante faktorer, eksempelvis områder hvor tilsynets kontrol fra lovgivers side er tillagt særlig vægt, såsom reglerne om videregivelse og udveksling af oplysninger.

Områder, hvor der vurderes at være en lav risiko for fejl, kontrolleres som hovedregel en gang hvert tredje år med henblik på at skabe fuldstændighed i kontrollen af CFCS og sikre, at vurderingen af risiko for fejl på området fortsat er retvisende.

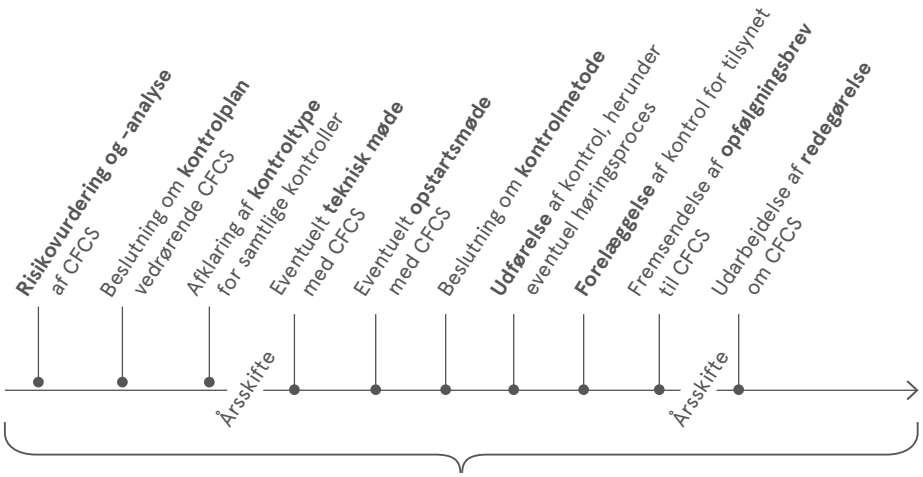
Tilsynets kontroller **2)** udføres løbende hen over året på baggrund af tilsynets beslutning om kontrolplan vedrørende CFCS. Tilsynet fastlægger ikke metoder for de enkelte kontroller i forbindelse med udarbejdelsen af risikovurderinger og -analyser, hvorfor metodevalget skal afklares forud for igangsættelse af en specifik kontrol.

Tilsynet benytter sig af en række forskellige metoder i kontrollen af de enkelte områder, heriblandt fuldstændig kontrol, tilfældige eller målrettede stikprøver, indholdsscreening, inspektioner og interviewbaserede kontroller.

Tilsynets valg af kontrolmetode sker på baggrund af en konkret risikovurdering af kontrolområdet, erfaringer fra tidligere kontroller samt de faktiske forhold, som tilsynet konstaterer i forbindelse med den specifikke kontrol. I den sammenhæng afholder tilsynet forud for en kontrol af ikke tidligere kontrollerede områder tekniske møder og opstartsmøder med relevante medarbejdere i CFCS med henblik på at sikre en tilstrækkelig teknisk forståelse af området, således at kontrollen kan tilpasses og gennemføres hensigtsmæssigt.

Endelig foretager tilsynet **3)** verificering ved løbende kortlægning af CFCS' it-infrastruktur på server-, komponent- og applikationsniveau med henblik på at kunne foretage fuldstændige risikovurderinger af samtlige processer og systemer i centret. Formålet med verificeringen er at sikre, at tilsynets kontrol beror på oplysninger fra CFCS, hvis rigtighed tilsynet har efterprøvet.

Tilsynets virksomhed forløber på følgende måde:



Løbende verificering og kortlægning af it-landskaber med feedback til risikovurderinger og -analyser samt afklaring af kontrolmetode for de enkelte kontroller

Tilsynets direkte adgang til CFCS' systemer sikrer, at centret ikke kan forudse, hvilke sager og oplysninger der bliver genstand for tilsynets kontrol. I nogle tilfælde er det imidlertid nødvendigt for tilsynet at varsle CFCS om tidspunktet og metoden for en kontrol, eksempelvis hvis tilsynet skal have adgang til særlige fysiske lokaliteter eller skal interviewe specifikke medarbejdere.

Tilsynet deler forud for påbegyndelsen af årets kontroller sin risikoanalyse og kontrolplan med CFCS med henblik på blandt andet at sikre åbenhed om tilsynets vurdering af forholdene i centret. Åbenheden giver endvidere CFCS mulighed for at tage højde for tilsynets kontrol i tilrettelæggelsen af centrets interne kontrol, hvilket bidrager til, at tilsynets kontrol og centrets interne kontrol samlet dækker en større del af centrets virksomhed. Endelig sikrer åbenheden, at CFCS kan afsætte tilstrækkelige ressourcer til at servicere tilsynet.

For yderligere information om tilsynets kontrolmetodik henvises til de af tilsynet udarbejdede standarder herfor, som findes på tilsynets hjemmeside.

1.2 Kontrol af CFCS i 2021

Med henblik på at kontrollere at CFCS i forbindelse med behandling af oplysninger om fysiske personer overholder reglerne i CFCS-loven, har tilsynet i 2021 foretaget kontrol af centrets

- behandling af oplysninger på sensornetværk (1.2.1),
- behandling af oplysninger i relation til indleverede medier (1.2.2),
- behandling af oplysninger i separate it-miljøer og analyseværktøjer (1.2.3),
- videregivelse af oplysninger til andre myndigheder, virksomheder og samarbejdspartnere (1.2.4),
- udveksling af oplysninger med den øvrige del af FE (1.2.5),
- interne kontrol (1.2.6) og
- opfølgning på tilsynets kontrol af CFCS i 2020 (1.2.7).

1.2.1 Kontrol af CFCS' behandling af oplysninger på sensornetværk

CFCS' sensornetværk overvåger internettrafik hos tilsluttede myndigheder og virksomheder. Sensorerne indeholder en række regler, der bruges til at genkende forsøg på cyberangreb. Når der via sensorerne registreres potentielt ondsindet trafik, som passer på en regel, modtager CFCS en alarm. Medarbejdere i CFCS henter derefter et relevant udsnit af internettrafikken med henblik på at foretage en undersøgelse af årsagen hertil. Data indhentet fra CFCS' sensornetværk må opbevares af centret mellem 13 måneder og fem år, jf. CFCS-lovens § 17, stk. 2.

Tilsynet har i 2021 foretaget kontrol af CFCS' behandling, herunder sletning, af oplysninger på centrets sensornetværk. Kontrollen blev foretaget ved gennemgang af et tilfældigt udvalgte sensorer på sensornetværket med henblik på at kontrollere, om oplysningerne blev slettet i overensstemmelse med CFCS-lovens § 17, stk. 2.

TILSYNETS BEMÆRKNINGER

Tilsynets kontrol af CFCS' anvendelse af centrets sensornetværk giver ikke anledning til bemærkninger.

1.2.2 Kontrol af CFCS' behandling af oplysninger i relation til indleverede medier

CFCS modtager løbende medier som computere, hardiske, mobiltelefoner mv. fra centrets kunder, PET, øvrige virksomheder og privatpersoner med henblik på teknisk analyse, herunder ved mistanke om kompromittering. Endvidere tilvejebringer CFCS medier i forbindelse med on-site assistance til kunder, hvor centret indhenter data, herunder images af computere, partitioner og logfiler.

Tilsynet har i 2021 foretaget kontrol af CFCS' behandling af oplysninger i relation til indleverede medier. Kontrollen blev foretaget ved inspektionsbesøg, hvor samtlige af de til CFCS indleverede medier blev kontrolleret.

TILSYNETS BEMÆRKNINGER

Tilsynet kan konstatere, at CFCS i 14 tilfælde ikke overholdt lovgivningens krav til sikkerhedsforanstaltninger i forbindelse med behandling af oplysninger, jf. CFCS-lovens § 18, stk. 1, og centrets interne retningslinjer, men at centrets håndtering af eksterne medier i øvrigt var tilrettelagt i overensstemmelse med lovgivningens krav.

Efter tilsynets vurdering skyldtes 13 af ovennævnte tilfælde, at der i CFCS' interne retningslinjer var uklarhed om, hvorvidt der skulle ske selvstændig registrering af 13 separat opbevarede simkort fra 13 indleverede routere, der i øvrigt var registreret i overensstemmelse med centrets interne retningslinjer. Tilsynet har efterfølgende noteret sig, at CFCS har præciseret de interne retningslinjer med henblik på at imødegå fremtidige fejl. Det sidste tilfælde skyldtes, at et en indleveret telefon manglede en påføring af et sagsnummer og dermed ikke var registreret i overensstemmelse med CFCS' interne retningslinjer.

1.2.3 Kontrol af CFCS' behandling af oplysninger på separate it-miljøer og analyseværktøjer

CFCS anvender en række separate it-miljøer og analyseværktøjer i forbindelse med centrets tekniske analyse af angreb og malware. CFCS behandler og lagrer sensordata i disse it-miljøer og analyseværktøjer i forbindelse med centrets analyse heraf.

Tilsynet har i 2021 foretaget kontrol af CFCS' behandling af oplysninger på et separat it-miljø og to analyseværktøjer.

TILSYNETS BEMÆRKNINGER

Tilsynets kontrol af CFCS' behandling af oplysninger på separate it-miljøer og analyseværktøjer giver ikke anledning til bemærkninger.

1.2.4 Kontrol af CFCS' videregivelse af oplysninger til andre myndigheder, virksomheder og samarbejdspartnere

CFCS foretager som led i varetagelsen af sine opgaver løbende videregivelse af oplysninger til andre myndigheder, virksomheder og samarbejdspartnere. CFCS kan blandt andet under særlige omstændigheder videregive oplysninger, som i forbindelse med en sikkerhedshændelse er indhentet fra centrets sensornetværk hos tilsluttede myndigheder, jf. CFCS-lovens § 16.

Tilsynet har i 2021 foretaget kontrol af CFCS' videregivelse af oplysninger. Kontrollen blev foretaget ved gennemgang af udvalgte dele af CFCS udgående kommunikation.

TILSYNETS BEMÆRKNINGER Tilsynets kontrol af CFCS' videregivelse af oplysninger giver ikke anledning til bemærkninger.

1.2.5 Kontrol af CFCS' udveksling af oplysninger med den øvrige del af FE

CFCS er organisatorisk en del af FE, og derfor er den interne udveksling af oplysninger mellem centret og de øvrige dele af FE ikke omfattet af CFCS-lovens regler om videregivelse. Forsvarsministeriet har i cirkulære nr. 9741 af 21. august 2019 om behandling af data i og fra Center for Cybersikkerheds netsikkerhedstjeneste (CFCS-cirkulæret) fastsat regler for udveksling af oplysninger fra CFCS til FE.

Tilsynet har i 2021 foretaget kontrol af CFCS' udveksling af oplysninger med den øvrige del af FE. Kontrollen blev foretaget ved gennemgang af adgangsbegrænsninger af en række sager i ét af CFCS' journalsystemer, der tillige anvendes af den øvrige del af FE.

TILSYNETS BEMÆRKNINGER Tilsynets kontrol af CFCS' udveksling af data indeholdende personoplysninger, der stammer fra indgreb i meddelelseshemmeligheden, med den øvrige del af FE, giver ikke anledning til bemærkninger.

1.2.6 Kontrol af CFCS' interne kontrol

CFCS foretager løbende intern kontrol af centrets overholdelse af konkrete dele af CFCS-loven. Til brug for tilrettelæggelsen af den interne kontrol udarbejder CFCS årligt en risiko- og væsentlighedsvurdering vedrørende centrets overholdelse af lovkrav samt en plan for den interne kontrol i det følgende år. CFCS orienterer løbende tilsynet om tilrettelæggelsen af den interne kontrol samt resultatet heraf, herunder ved fremsendelse af centrets risikoanalyse og kontrolplan.

Med henblik på kontrol heraf foretog tilsynet i 2021 en gennemgang af resultatet af CFCS' interne kontrol i 2020, samt centrets risiko- og væsentlighedsvurdering, herunder kontrolplanen for 2021.

TILSYNETS BEMÆRKNINGER Tilsynets kontrol af CFCS' interne kontrol giver ikke anledning til bemærkninger.

1.2.7 Opfølgning på tilsynets kontrol af CFCS i 2020

Tilsynet foretager årligt kontrol af, at CFCS har foretaget de handlinger, som centret på baggrund af tilsynets kontrol i det foregående år har tilkendegivet at ville gennemføre.

TILSYNETS BEMÆRKNINGER Tilsynets opfølgning på kontrollen af CFCS i 2020 giver ikke anledning til bemærkninger.

2. Rammerne for sletning af data indhentet fra centrets sensornetværk i CFCS-lovens § 17

Med henblik på at opdage cyberangreb og forsøg på cyberangreb driver CFCS et sensornetværk, der anvendes til at monitorere internetforbindelsen hos et antal tilsluttede myndigheder, herunder flere ministerier og offentlige myndigheder, og virksomheder. Det nuværende sensornetværk er egenudviklet og består af hardwareenheder placeret hos de tilsluttede myndigheder og virksomheder.

Sensornetværket indeholder en række regler, der bruges til at genkende forsøg på cyberangreb. Det kan være IP-adresser eller internetdomæner, der bliver brugt af en hackergruppe, eller digitale fingeraftryk af filer, der indeholder malware.

Når der registreres potentielt skadelig trafik, der passer på en regel, modtager CFCS en alarm. På baggrund af en alarm kan CFCS vælge at hente sensordata fra den enkelte myndighed og foretage en nærmere analyse heraf. I de tilfælde, hvor CFCS' analyse ikke viser tegn på, at der skulle være tale om en sikkerhedshændelse, betegnes det som en "falsk positiv".

I 2021 behandlede CFCS 5.677 sikkerhedshændelser, hvoraf 5.298 af sikkerhedshændelserne af centret blev vurderet som havende ingen eller begrænset effekt, hvilket blandt andet dækker over falske positive alarmer fra centrets sensornetværk (se afsnit 4).

Hvad er sensordata?

Sensordata er en samlebetegnelse for data, som er indhentet via CFCS' sensornetværk. Sensordata dækker over to typer af data, som er reguleret selvstændigt i CFCS-loven.

Pakkedata: Indholdet af den kommunikation, der transmitteres. Dette kan eksempelvis være indholdet af en e-mail fra en borger eller virksomhed, som er sendt til eller fra den tilsluttede myndighed eller virksomhed.

Trafikdata: Data som behandles med henblik på transmittere pakkedata. Trafikdata kan være oplysninger om afsender og modtager for en transmission, eksempelvis IP-adresser. I andre sammenhænge anvendes betegnelsen metadata ofte om det, som i CFCS-loven betegnes trafikdata.

2.1 Tilsynets kontrol af CFCS' sletning af sensordata

Tilsynet foretog i 2019 kontrol af CFCS' tilvejebringelse af oplysninger fra centrets sensornetværk på baggrund af alarmer samt efterfølgende behandling af indhentet sensordata (se tilsynets redegørelse for 2019, afsnit 1.2.1).

Formålet med kontrollen var blandt andet at sikre, at data indhentet fra CFCS' sensornetværk blev slettet i overensstemmelse med CFCS-lovens regler.

Tilsynet foretog en kontrol af CFCS' sletning af pakkedata i tilfælde, hvor centret havde afsluttet behandlingen af den alarm, som havde givet anledning til, at pakkedata var blevet hentet fra sensornetværket.

Tilsynet konstaterede på baggrund af kontrollen, at CFCS i 67 procent af de udtrukne tilfælde ikke havde foretaget sletning af den indhentede pakkedata, på trods af at behandlingen af alarmen var afsluttet.

Det var tilsynets vurdering, at CFCS' fortsatte opbevaring af pakkedata i de pågældende tilfælde var i strid med CFCS-lovens § 17, stk. 1, hvoraf det fremgår, at centeret er forpligtet til at slette blandt andet pakkedata, når formålet med behandlingen er opfyldt.

CFCS var ikke enig i tilsynets vurdering, idet centret vurderede, at formålet med behandlingen heraf endnu ikke var opfyldt. Dette skyldtes, at CFCS vurderede, at der fortsat var behov for at kunne fremfinde tidligere behandlet pakkedata, blandt andet med henblik på at kunne identificere om tidligere aktører på ny er aktive, eller om data, der ser mistænkelig ud, tidligere har været analyseret som falske alarmer.

Tilsynet lagde ved sin vurdering særligt vægt på ordlyden af CFCS-lovens § 17 og forarbejderne til loven.

Følgende fremgår af bemærkningerne til CFCS-lovens § 17:

> *"Den foreslåede § 17 fastsætter de tidsmæssige rammer for Center for Cybersikkerheds opbevaring af de data, der behandles i medfør af det foreslåede kapitel 4 og dermed behandles på baggrund af indgreb i meddelelseshemmeligheden.*
>
> *(...)*
>
> *Bestemmelsen er en delvis videreførelse af GovCERT-lovens § 4, stk. 2-4. Efter det foreslåede stk. 1 vil data skulle slettes, når formålet med behandlingen er opfyldt, hvilket er en videreførelse af GovCERT-lovens § 4, stk. 2, idet bestemmelsen dog foreslås udvidet til at omfatte alle former for data, der behandles på baggrund af indgreb i meddelelseshemmeligheden.* ***Der vil på den baggrund ske en løbende vurdering af de behandlede data*** *med henblik på at sikre, at* ***data, der ikke længere er relevante i forhold til netsikkerhedstjenestens formål og aktiviteter****, straks slettes."*

Da CFCS-lovens § 17, stk. 1, er en videreførsel af GovCERT-lovens § 4, stk. 2-4, lagde tilsynet ved sin vurdering tillige vægt på forarbejderne til GovCERT-lovens § 4, hvoraf følgende fremgår:

> *"Opbevaringsperioden for indsamlede oplysninger om de tilsluttede myndigheders ind- og udgående internetkommunikation vil højst være tre år for så vidt angår pakke- og trafikdata, der knytter sig til en sikkerhedshændelse. Opbevaringsperioden*

påregnes dog i de mange tilfælde at være væsentligt kortere, ***idet GovCERT er forpligtet til at slette data, så snart data ikke længere er relevant*** *i forhold til GovCERT´s formål og aktiviteter."*

Derudover fremgår følgende af de almindelige bemærkninger til GovCERT-loven:

"Pakkedata vil blive slettet umiddelbart efter GovCERT's analyse, hvis denne ikke viser tegn på en sikkerhedshændelse. *Analyseret pakkedata vil således kun blive opbevaret i GovCERT's system til at registrere sikkerhedshændelser, hvis data er knyttet til en sikkerhedshændelse."*

Det var på den baggrund tilsynets vurdering, at CFCS-lovens § 17 er udtryk for et dataminimeringsprincip, således at CFCS i videst muligt omfang skal slette pakkedata, når centret ikke længere har behov for at behandle den pågældende data.

Tilsynet bemærkede i forbindelse med kontrollen, at et generelt behov for at kunne fremfinde tidligere behandlet pakkedata, uanset om pakkedata, vedrører eller ikke vedrører en sikkerhedshændelse efter tilsynets vurdering ikke er en tilstrækkelig begrundelse for at undlade sletning efter CFCS-lovens § 17, stk. 1.

Tilsynet bemærkede endvidere, at en udstrækning af slettefristen i CFCS-lovens § 17, stk. 1, til i alle tilfælde at være sammenfaldende med de absolutte slettefrister i CFCS-lovens § 17, stk. 2, vil betyde, at CFCS-lovens § 17, stk. 1, ikke har et selvstændigt indhold.

CFCS indbragte spørgsmålet for forsvarsministeren den 11. august 2020. Tilsynet blev på møde den 11. august 2021 mundtligt orienteret om forsvarsministerens afgørelse, og Forsvarsministeriet fremsendte den 1. november 2021 skriftligt afgørelsen til tilsynet.

2.2 Forsvarsministerens afgørelse

Forsvarsministeren vurderer, at sensordata, hvor CFCS efter endt analyse vurderer, at der er tale om en falsk positiv alarm, og som derfor efter centrets opfattelse ikke vedrører en sikkerhedshændelse, ikke skal slettes i henhold til CFCS-lovens § 17, stk. 1, idet formålet med behandlingen ikke er opfyldt.

Dette skyldes, at CFCS' analyse alene er sket på baggrund af de metoder og værktøjer, der var kendt på analysetidspunktet, hvorfor centret skal have mulighed for at foretage nye analyser af den pågældende sensordata, hvis ny viden eller teknologi bliver tilgængelig, ligesom centret skal kunne foretage bagudrettede analyser af sensordata i forbindelse med nye sikkerhedshændelser.

Foruden hensynet til CFCS' mulighed for at foretage analyse af tidligere indhentet sensordata, lægger forsvarsministeren i sin afgørelse vægt på CFCS' muligheder for at tegne et normalbillede af internetaktiviteten hos tilsluttede myndigheder.

I tilfælde, hvor CFCS' analyse af sensordata viser, at der har været tale om en sikkerhedshændelse, vil data alene skulle slettes i henhold til CFCS-lovens § 17, stk. 1, såfremt centret vurderer, at det konkrete data ikke vil være relevant for CFCS' fremtidige muligheder for at opdage, analysere og bidrage til at imødegå cyberangreb. CFCS er imidlertid tillagt en betydelig grad af skøn i forhold til, hvornår formålet med behandlingen af data er opfyldt.

Forsvarsministeren vurderer derfor, at CFCS-lovens § 17, stk. 1, i forhold til sensordata har et meget begrænset anvendelsesområde. Bestemmelsens primære anvendelsesområde er derimod de øvrige former for data, der er omfattet af CFCS-lovens kapitel 4.

Udgangspunktet vil derfor være, at sensordata, som knytter sig til en sikkerhedshændelse, opbevares af CFCS i 5 år. Sensordata, som ikke knytter sig til en sikkerhedshændelse, opbevares som udgangspunkt i 13 måneder – dog i 3 år når data stammer fra myndigheder og virksomheder, som i særlig grad beskæftiger sig med eller har betydning for udenrigs-, sikkerheds- og forsvarspolitiske forhold.

Andre praktiske eller kapacitetsmæssige forhold kan imidlertid føre til, at sensordata slettes inden udløbet af slettefristerne.

2.3 Tilsynets bemærkninger

Tilsynet vil fremover lægge forsvarsministerens fortolkning af CFCS-lovens § 17, stk. 1, til grund i forbindelse med kontrollen af CFCS.

3. Eksempler på CFCS' håndtering af cyberangreb

Ifølge forarbejderne til CFCS-loven skal tilsynets årlige redegørelse om sin virksomhed vedrørende CFCS blandt andet indeholde en fuldt ud anonymiseret beskrivelse af et eller flere konkrete cyberangreb.

CFCS har bidraget med følgende beskrivelse af cyberangreb i 2021:

Center for Cybersikkerheds (CFCS) Netsikkerhedstjeneste har til opgave at opdage, analysere og bidrage til at imødegå it-sikkerhedshændelser hos de offentlige myndigheder og private virksomheder, der er tilsluttet sensornetværket. Netsikkerhedstjenesten består af flere organisatoriske enheder i CFCS.

Netsikkerhedstjenesten inkluderer CFCS' Cybersituationscenter, der foruden de tilsluttede kunder også har et særligt fokus på at analysere og informere om aktuelle cyberangreb, som påvirker dansk kritisk infrastruktur, herunder de seks samfundsvigtige sektorer i Danmark.

I 2021 har Netsikkerhedstjenesten håndteret og observeret en række it-sikkerhedshændelser. Størstedelen af disse hændelser omhandlede primært rekognosceringsforsøg, forskellige former for social engineering samt forsøg på udnyttelser af sårbarheder og fejlkonfigurationer i software, der er eksponeret mod internettet. CFCS har derudover observeret og behandlet et antal angrebsforsøg med relation til ransomware.

Baseret på CFCS' observationer anses angrebsforsøg via phishingmails fortsat som en alvorlig trussel mod centrets kunder. Dette kan eksempelvis være mails fra forskellige ondsindede aktører, der forsøger at lokke modtageren til at aktivere eller tilgå indhold i mailen, som enten kan føre til inficeringer eller som forsøger at franarre adgangsoplysninger fra ofret.

Desuden har CFCS som nævnt observeret forskellige typer forsøg på at udnytte eventuelle fejlkonfigurationer og sårbarheder i softwaretjenester, som kunderne har eksponeret mod internettet. Dette indebærer eksempelvis også regulære brute force-relaterede angrebsforsøg rettet mod eksponerede it-systemer hos kunderne, som angriberen forsøger at tiltvinge sig adgang til.

4. Statistik vedrørende CFCS' behandling af oplysninger

Det fremgår af forarbejderne til CFCS-loven, at tilsynets årlige redegørelse om sin virksomhed vedrørende CFCS skal indeholde statistiske oplysninger om centrets behandling af personoplysninger, herunder oplysninger om antallet af modtagne klagesager i såvel centret som tilsynet, oplysninger om antallet af aktindsigtssager og afgørelsen af disse samt oplysninger om antallet af sager med relation til sikkerhedshændelser, der er behandlet i centret.

Redegørelsen skal endvidere indeholde statistik over antallet af tilfælde, hvor en analytiker fra CFCS på baggrund af indgreb i meddelelseshemmeligheden har foretaget en analyse af data. Denne statistik skal indeholde en overordnet kategorisering af, hvor alvorlige disse tilfælde har været.

CFCS har bidraget med følgende data for 2021:

TABEL 1

Modtagne klagesager over CFCS' behandling af personoplysninger

Kategorier	2021
Klager til CFCS over behandling af personoplysninger	0
Klagesager modtaget i tilsynet	0

TABEL 2

Aktindsigtssager

Kategorier	2021
Fuld aktindsigt	0
Delvis aktindsigt	1
Afslag på aktindsigt	3
Ingen dokumenter lokaliseret til at give eller afslå aktindsigt i	2
Total	**6**

TABEL 3

Sikkerhedshændelser* efter alvorlighedsgrad

Kategorier	2021
Alvorlige cyberangreb	2
Større cyberangreb	7
Moderate cyberangreb	23
Mindre cyberangreb	347
Ingen/begrænset effekt**	5.298
Total	**5.677**

* Sikkerhedshændelser defineres i overensstemmelse med § 2, nr. 1, i lov om Center for Cybersikkerhed.
** Kategorien "Ingen/begrænset effekt" inkluderer alle sikkerhedshændelser, som ikke har haft indvirkning på kunden.

TABEL 4

CFCS' videregivelse* og udveksling af oplysninger

Kategorier	2021
Videregivelser	67
Udvekslinger	15

* Antallet af CFCS' netsikkerhedstjenestes videregivelser af oplysninger, herunder oplysninger, der stammer fra indgreb i meddelelseshemmeligheden, omfatter samtlige videregivne oplysninger, herunder om fysiske og juridiske personer, samt oplysninger, der ikke er personhenførbare. Se desuden tilsynets kontrol heraf, jf. afsnit 1.2.4.

Appendiks

1. Om Center for Cybersikkerhed

Center for Cybersikkerhed (CFCS) blev oprettet i 2012 som en del af Forsvarets Efterretningstjeneste (FE) og har som hovedopgave at være

- statslig og militær varslingstjeneste for internettrusler,
- national it-sikkerhedsmyndighed (bortset fra Justitsministeriets område, hvor Politiets Efterretningstjeneste (PET) varetager opgaven) og
- myndighed for informationssikkerhed og beredskab på teleområdet.

Det er CFCS' opgave som statslig og militær varslingstjeneste for internettrusler at understøtte et højt informationssikkerhedsniveau i den informations- og kommunikationsteknologiske infrastruktur, som samfundsvigtige funktioner er afhængige af. Denne opgave løses blandt andet ved, at CFCS' netsikkerhedstjeneste opdager, analyserer og bidrager til at imødegå avancerede cyberangreb hos Forsvaret samt de statslige myndigheder og virksomheder, der er tilsluttet centrets sensornet.

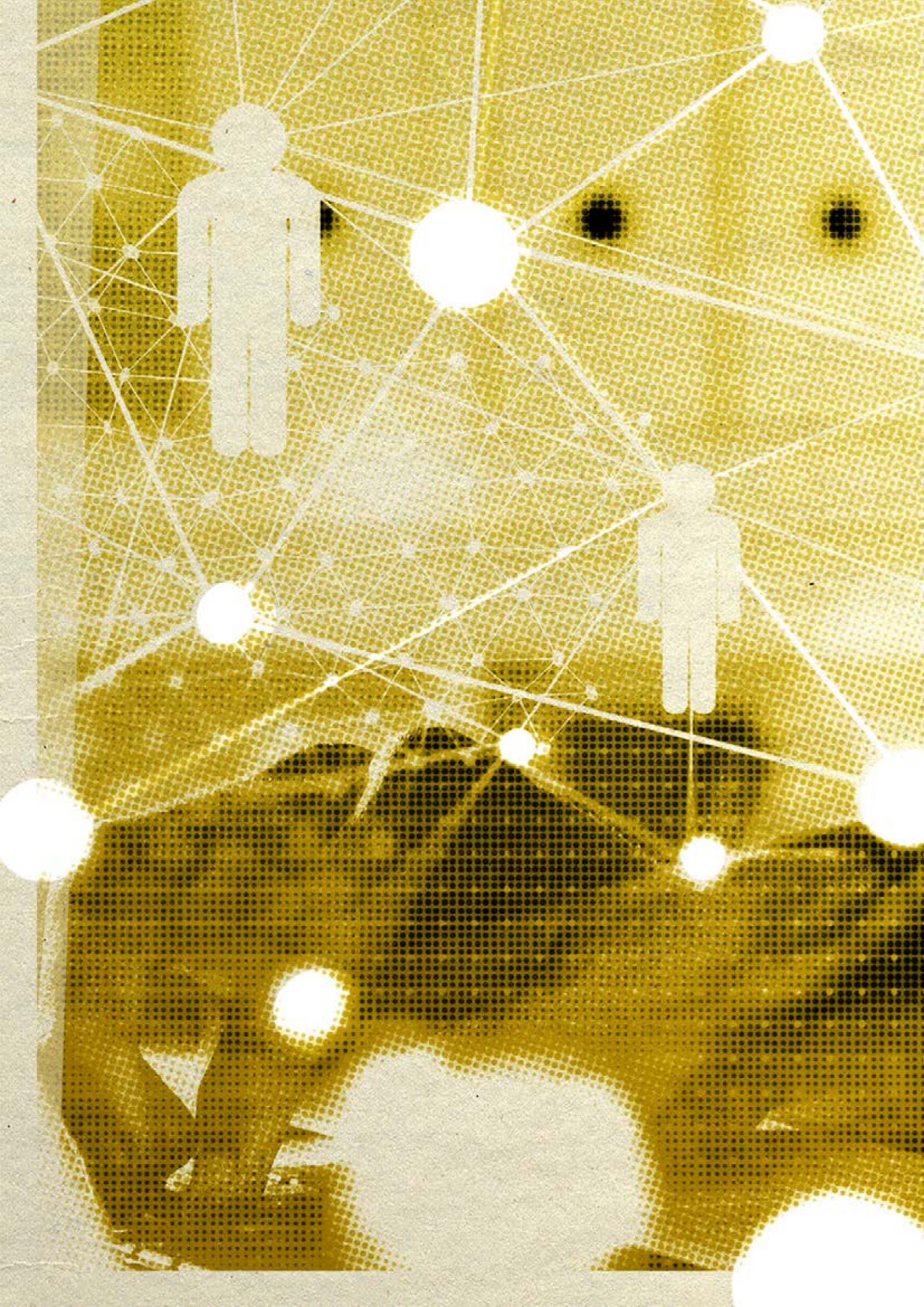
CFCS' opgave som national it-sikkerhedsmyndighed indebærer, at centret oplyser, vejleder og rådgiver danske myndigheder og virksomheder om it-sikkerhed og fungerer som nationalt kompetencecenter på cybersikkerhedsområdet. Som national it-sikkerhedsmyndighed er det tillige CFCS' opgave at sikkerhedsgodkende og føre tilsyn med klassificerede produkter, systemer og installationer inden for informations- og kommunikationsteknologi.

CFCS' varetagelse af opgaven som myndighed for informationssikkerhed og beredskab på teleområdet indebærer, at centret blandt andet fører tilsyn på området og rådgiver samfundets beredskabsaktører om teleberedskab. Herunder udsteder CFCS med bemyndigelse i lov om net- og informationssikkerhed (herefter NIS-loven) bekendtgørelser og har til opgave at føre tilsyn på området samt på overordnet niveau at koordinere håndteringen af særlige trusler, som kan påvirke informationssikkerheden i telesektoren.

De juridiske rammer for CFCS' virksomhed følger i det væsentlige af CFCS-loven med tilhørende bekendtgørelse og cirkulære samt NIS-loven.

CFCS-loven regulerer blandt andet centrets opgaver samt indgreb i meddelelseshemmeligheden, behandling, analyse, videregivelse og sletning af personoplysninger. Med loven er det yderligere bestemt, at Tilsynet med Efterretningstjenesterne, der som et uafhængigt kontrolorgan fører tilsyn med PET og FE, tillige skal føre tilsyn med, at CFCS' behandling af oplysninger om fysiske personer er i overensstemmelse med lovgivningen.

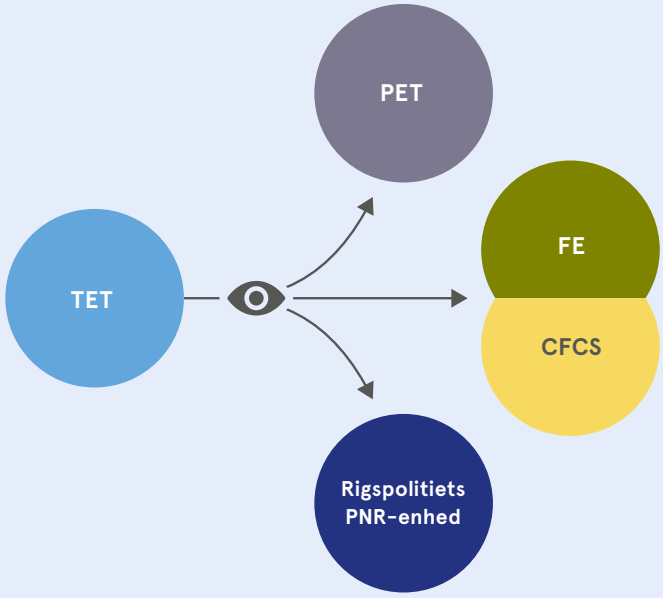
CFCS er tillige undergivet ekstern kontrol af Forsvarsministeriet, domstolene og Folketingets Ombudsmand.



Appendiks

2. Tilsynet med Efterretningstjenesterne

Tilsynet er et særligt uafhængigt kontrolorgan, der fører tilsyn med, at PET, FE, CFCS og Rigspolitiets PNR-enhed (RPNR) behandler personoplysninger i overensstemmelse med lovgivningen.



Tilsynet udøver sine funktioner i fuld uafhængighed og er således ikke undergivet tjenestebefalinger fra Forsvarsministeriet eller andre administrative myndigheder med hensyn til udøvelsen af sin virksomhed.

Tilsynet består af fem medlemmer, der er udpeget af justitsministeren efter forhandling med forsvarsministeren. Formanden, der skal være landsdommer, er udpeget efter indstilling fra præsidenterne for Østre Landsret og Vestre Landsret, mens de øvrige medlemmer er udpeget efter drøftelser med Folketingets Udvalg vedrørende Efterretningstjenesterne.

Medlemmerne var ved udgangen af 2021:

- Landsdommer Michael Kistrup, Østre Landsret (formand)
- Juridisk chef Pernille Christensen, Kommunernes Landsforening
- Professor Henrik Udsen, Københavns Universitet
- Professor Rebecca Adler-Nissen, Københavns Universitet
- Koncerndirektør David Hellemann, Nykredit (udtrådt pr. 1. februar 2022)

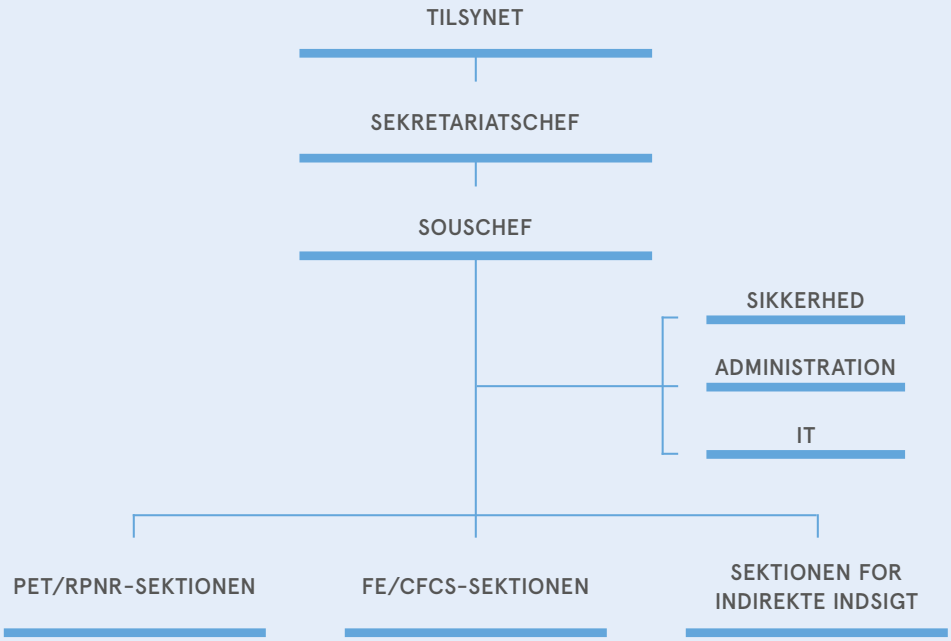
Medlemmerne udpeges for en periode på fire år med mulighed for genbeskikkelse for yderligere fire år. Ved tilsynets etablering i 2014 blev to medlemmer udpeget for to år med mulighed for genbeskikkelse for yderligere fire år med henblik på at sikre mod en

samtidig og fuldstændig udskiftning af tilsynets medlemmer, idet de efterfølgende funktionsperioder er forskudt to år i forhold til hinanden.

Tilsynet bistås af et sekretariat, der alene er undergivet tilsynets instruktion. Tilsynet bestemmer selv, hvem der skal ansættes til sekretariatet, herunder hvilken uddannelsesmæssig baggrund og øvrige kvalifikationer de pågældende skal have. Ved udgangen af 2021 bestod sekretariatet af en sekretariatschef, der varetager den daglige ledelse af sekretariatet, en souschef, tre jurister, to it-konsulenter og en kontorfunktionær.

Sekretariatet er opdelt i sektioner, der beskæftiger sig med henholdsvis PET/RPNR, FE/CFCS og anmodninger om indirekte indsigt. Med henblik på at sikre faglig koordinering og erfaringsudveksling arbejder tilsynets medarbejdere på tværs af sektionerne.

Organisation 2021



2.1 Tilsynets opgaver i forhold til CFCS

Ifølge CFCS-loven skal tilsynet efter klage eller af egen drift påse, at CFCS behandler oplysninger om fysiske personer i overensstemmelse med de nærmere bestemmelser herom i CFCS-loven samt regler udstedt i medfør heraf. Tilsynet påser, at CFCS overholder lovens regler om

- indgreb i meddelelseshemmeligheden,
- behandling af personoplysninger i centret,
- analyse, videregivelse og sletning af data og
- krav til sikkerhedsforanstaltninger i forbindelse med centrets behandling af personoplysninger.

Tilsynets opgave er at føre legalitetskontrol med, at CFCS behandler oplysninger om fysiske personer i overensstemmelse med lovgivningen, og tilsynet skal således ikke påse, hvorvidt centret udfører sine opgaver på en hensigtsmæssig måde.

Tilsynet afgør selv intensiteten af sin kontrol, herunder i hvilket omfang kontrollen skal være fuldstændig eller stikprøvevis, hvilke sagsområder der særskilt skal prioriteres, og i hvilket omfang tilsynet vil tage sager op af egen drift. Der er ikke givet nærmere retningslinjer for tilsynets udførelse af sin kontrol.

2.2 Tilsynets adgang til oplysninger i CFCS

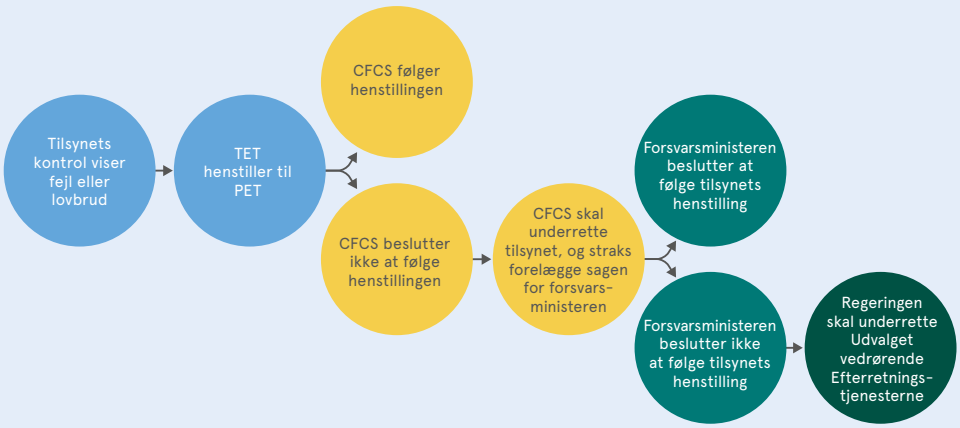
Tilsynet kan hos CFCS kræve enhver oplysning og alt materiale, der er af betydning for tilsynets virksomhed, og tilsynet har til enhver tid adgang til alle lokaler, hvorfra der er adgang til de oplysninger, som behandles, eller hvor tekniske hjælpemidler anvendes. Tilsynet kan endvidere afkræve CFCS skriftlige udtalelser om faktiske og retlige forhold af betydning for tilsynets kontrolvirksomhed, ligesom tilsynet kan anmode om, at en repræsentant for centret er til stede med henblik på at redegøre for de behandlede sager.

CFCS har stillet lokaler til rådighed for tilsynet, hvorfra tilsynet på egen hånd kan foretage søgninger i centrets it-systemer.

2.3 Tilsynets reaktionsmuligheder

Tilsynet har ikke kompetence til at påbyde CFCS bestemte foranstaltninger i forhold til behandling af oplysninger. Tilsynet kan derimod afgive udtalelser over for CFCS, hvori tilsynet blandt andet kan tilkendegive sin opfattelse af, om centret overholder reglerne om behandling af personoplysninger. Hvis CFCS undtagelsesvis måtte beslutte ikke at følge en henstilling i en udtalelse fra tilsynet, skal centret underrette tilsynet herom og straks forelægge sagen for forsvarsministeren til afgørelse.

Tilsynets reaktionsmuligheder



Tilsynet skal underrette forsvarsministeren om forhold, som ministeren efter tilsynets opfattelse bør have kendskab til.

Tilsynet afgiver en årlig redegørelse om sin virksomhed til forsvarsministeren. Redegørelsen, der desuden offentliggøres, giver information om karakteren af det tilsyn, der udøves med CFCS. Det fremgår således af forarbejderne til loven, at sigtet med den årlige redegørelse er at give information om karakteren af det tilsyn, der udøves vedrørende CFCS, herunder en generel beskrivelse af, hvilke forhold tilsynet måtte have valgt særligt at interessere sig for. Redegørelsen skal indeholde statistiske oplysninger om CFCS' behandling af personoplysninger, herunder oplysninger om antallet af modtagne klagesager i såvel centret som tilsynet, oplysninger om antallet af aktindsigtssager og afgørelsen af disse samt oplysninger om antallet af sager med relation til sikkerhedshændelser, der er behandlet i centret. Tilsynet vil også skulle medtage oplysninger om, i hvor mange tilfælde tilsynet har fundet, at CFCS' behandling af personoplysninger ikke har været i overensstemmelse med reglerne. Redegørelsen skal ligeledes indeholde en fuldt ud anonymiseret beskrivelse af et eller flere konkrete cyberangreb samt en statistik over antallet af tilfælde, hvor en analytiker fra CFCS på baggrund af indgreb i meddelelseshemmeligheden har foretaget en analyse af data. Denne statistik skal desuden indeholde en overordnet kategorisering af, hvor alvorlige disse tilfælde har været.

Tilsynet afgav senest en årlig redegørelse om sin virksomhed til forsvarsministeren i august 2021. Redegørelsen blev offentliggjort i september 2021.

Appendiks 3. Retsgrundlag

1) Lov om Center for Cybersikkerhed (CFCS) (lovbekendtgørelse nr. 836 af 7. august 2019) (CFCS-loven)

2) Forsvarsministeriets cirkulære om behandling af data i og fra Center for Cybersikkerheds netsikkerhedstjeneste (cirkulære nr. 9741 af 21. august 2019) (CFCS-cirkulæret)

3) Anordning nr. 1658 af 20. november 2020 om ikrafttræden for Grønland af lov om Center for Cybersikkerhed

3.1 CFCS' netsikkerhedstjeneste

3.1.1 Om CFCS' netsikkerhedstjeneste, jf. CFCS-lovens § 3

Det følger af lovens § 3, at CFCS' netsikkerhedstjenestes opgave er at opdage, analysere og bidrage til at imødegå sikkerhedshændelser hos tilsluttede myndigheder og virksomheder. Det er de øverste statsorganer samt statslige myndigheder, der efter anmodning kan blive tilsluttet netsikkerhedstjenesten, mens regioner og kommuner samt virksomheder, der er beskæftiget med samfundsvigtige funktioner, efter anmodning kan blive tilsluttet netsikkerhedstjenesten, såfremt CFCS konkret vurderer, at tilslutningen vil kunne bidrage til at understøtte et højt informationssikkerhedsniveau i samfundet. I særlige tilfælde kan CFCS påbyde virksomheder, der har særlig samfundsvigtig karakter, samt regioner og kommuner at blive tilsluttet netsikkerhedstjenesten.

CFCS' netsikkerhedstjeneste er betegnelsen for centret samlede aktiviteter i forbindelse med at opdage, analysere og bidrage til at imødegå sikkerhedshændelser, herunder CERT-aktiviteterne på det civile område (GovCERT), CERT-aktiviteterne på det militære område (MILCERT), sikkerhedstekniske aktiviteter (f.eks. analyse af malware) og støttefunktioner. Ved myndigheders og virksomheders tilslutning til netsikkerhedstjenesten bliver der indgået en tilslutningsaftale, der nærmere regulerer specifikke forhold i relationen mellem netsikkerhedstjenesten og den enkelte tilsluttede myndighed eller virksomhed. På Forsvarsministeriets område er det den militære it-sikkerhedsmyndighed, som pålægger myndigheder at blive tilsluttet netsikkerhedstjenesten, og på dette område indgås ikke tilslutningsaftaler.

3.2 Indgreb i meddelelseshemmeligheden og edition

3.2.1 Om indgreb i meddelelseshemmeligheden, jf. CFCS-lovens §§ 4-6 c

CFCS-lovens § 4 indebærer, at CFCS' netsikkerhedstjeneste uden retskendelse kan behandle pakkedata, trafikdata og stationære data hidrørende fra tilsluttede myndigheder og virksomheder med henblik på at understøtte et højt informationssikkerhedsniveau i samfundet. Ved pakkedata forstås indholdet af kommunikation, der transmitteres gennem digitale netværk eller tjenester, jf. lovens § 2, nr. 2, og ved trafikdata forstås data, som behandles med henblik på at transmittere pakkedata, jf. lovens § 2, nr. 3. Ved stationære data forstås data, som opbevares på servere, cloudtjenester, pc'er, lagerenheder, netværksenheder, mobile enheder og tilsvarende, jf. lovens § 2, nr. 3.

Det følger af lovens § 5, at CFCS ved en begrundet mistanke om en sikkerhedshændelse uden retskendelse kan behandle stationære data fra en myndighed eller virksomhed, som ikke er tilsluttet netsikkerhedstjenesten, når

1) myndigheden eller virksomheden har anmodet CFCS om bistand, stillet de stationære data til rådighed og givet skriftligt samtykke til behandlingen, og

2) behandlingen vurderes at kunne bidrage til at understøtte et højt informationssikkerhedsniveau i samfundet.

Det følger af lovens § 6, at CFCS efter aftale med en myndighed eller virksomhed, som er tilsluttet centrets netsikkerhedstjeneste, ved begrundet mistanke om en sikkerhedshændelse uden retskendelse kan blokere, omdanne eller omdirigere trafikdata, pakkedata og stationære data hidrørende fra netværk hos myndigheden eller virksomheden med henblik på at understøtte et højt informationssikkerhedsniveau i samfundet. Ved en konstateret sikkerhedshændelse kan CFCS slette stationære data, der har forårsaget sikkerhedshændelsen.

Efter lovens § 6 a kan CFCS gennemføre sikkerhedstekniske undersøgelser med henblik på at kunne rådgive myndigheder og virksomheder om forebyggelse af sikkerhedshændelser, når en myndighed eller virksomhed har anmodet centret herom. I forbindelse med en sikkerhedsteknisk undersøgelse kan CFCS uden retskendelse behandle trafikdata, pakkedata og stationære data hos myndigheden eller virksomheden, behandle offentligt tilgængelige data om myndigheden eller virksomheden og dennes medarbejdere og iværksætte forebyggelsesaktiviteter rettet mod udvalgte medarbejdere eller enheder i myndigheden eller virksomheden.

Efter lovens § 6 b kan CFCS med henblik på at opnå viden om angrebsaktørers metoder og værktøjer opsætte fiktive angrebsmål, såfremt opsætningen vurderes at kunne bidrage væsentligt til centrets muligheder for at understøtte et højt informationssikkerhedsniveau i samfundet. Såfremt angrebsaktører benytter et fiktivt angrebsmål til at deponere data, kan CFCS uden retskendelse behandle de deponerede data med henblik på at opdage, analysere og bidrage til at imødegå sikkerhedshændelser hos myndigheder og virksomheder eller informere borgere, myndigheder og virksomheder om, at de har været udsat for en sikkerhedshændelse.

Det følger af lovens § 6 c, at CFCS med henblik på at forhindre, standse eller begrænse en nært forestående eller igangværende sikkerhedshændelse kan gøre brug af domænenavne og tilsvarende it-infrastruktur, som anvendes eller har været anvendt af en angrebsaktør,

forudsat at disse er ledige til registrering. Såfremt CFCS i forbindelse med anvendelsen af it-infrastruktur modtager data fra tredjemand, kan centret uden retskendelse behandle de modtagne data med henblik på at opdage, analysere og bidrage til at imødegå sikkerhedshændelser hos myndigheder og virksomheder eller informere borgere, myndigheder og virksomheder om, at de har været udsat for en sikkerhedshændelse.

3.2.2 Om edition, jf. CFCS-lovens § 7

Med henblik på at afdække sikkerhedshændelser kan der efter lovens § 7 meddeles en juridisk eller fysisk person pålæg om at forevise eller udlevere oplysninger om brugeren af en e-mailkonto, ip-adresse eller et domænenavn, såfremt oplysningerne er undergivet den pågældendes rådighed, medmindre indgrebet står i misforhold til sagens betydning og det tab eller den ulempe, som indgrebet kan antages at medføre.

3.3 Behandling af personoplysninger

3.3.1 Om behandling af personoplysninger, jf. CFCS-lovens §§ 9-14

Efter lovens § 9 skal CFCS' indsamling af personoplysninger ske til udtrykkeligt angivne og saglige formål, og senere behandling må ikke være uforenelig med disse formål. Senere behandling af personoplysninger, der alene sker i historisk, statistisk eller videnskabeligt øjemed, anses ikke for uforenelig med de formål, hvortil oplysningerne er indsamlet. Personoplysninger, som behandles, skal være relevante og tilstrækkelige og ikke omfatte mere, end hvad der kræves til opfyldelse af de formål, hvortil oplysningerne indsamles, og de formål, hvortil oplysningerne senere behandles.

Behandling af personoplysninger må efter lovens § 10 kun finde sted, hvis

1) den pågældende person har givet sit udtrykkelige samtykke hertil,

2) behandlingen er nødvendig af hensyn til opfyldelsen af en aftale, som den pågældende person er part i, eller af hensyn til gennemførelse af foranstaltninger, der træffes på den pågældende persons anmodning forud for indgåelsen af en sådan aftale,

3) behandlingen er nødvendig af hensyn til udførelsen af en opgave i samfundets interesse,

4) behandlingen er nødvendig til beskyttelse af væsentlige hensyn til statens sikkerhed eller rigets forsvar,

5) behandlingen er nødvendig af hensyn til udførelsen af en opgave, der henhører under offentlig myndighedsudøvelse, som CFCS eller en tredjemand, til hvem oplysningerne videregives, har fået pålagt,

6) behandlingen er nødvendig for, at CFCS eller den tredjemand, til hvem oplysningerne videregives, kan forfølge en berettiget interesse, og hensynet til den pågældende person ikke overstiger denne interesse, eller

7) behandlingen vedrører personoplysninger, der er omfattet af kapitel 4 (indgreb i meddelelseshemmeligheden).

Lovens § 10, nr. 1, 2, 3, 5 og 6 er med sproglige tilpasninger identiske med de tilsvarende bestemmelser i Europa-Parlamentets og Rådets forordning 2016/679 artikel 6 og skal fortolkes i overensstemmelse med disse bestemmelsers forarbejder og relevante praksis. Anvendelse af bestemmelsens nr. 4 forudsætter, at der er fare for, at statens sikkerhed eller rigets forsvar vil lide skade, hvilket eksempelvis kan være tilfældet i forbindelse med cyberangreb mod danske myndigheders informationssystemer. Hensynet til statens sikkerhed eller rigets forsvar skal fortolkes i overensstemmelse med det tilsvarende udtryk i offentlighedslovens § 31. Med bestemmelsens nr. 7 fastsættes en generel hjemmel til at behandle personoplysninger, hvis de er omfattet af kapitel 4 (indgreb i meddelelseshemmeligheden), hvorved bemærkes, at der med lovens § 15 er fastsat nærmere rammer for analyse af pakkedata, der er omfattet af lovens §§ 4, 6 og 7, mens der i lovens § 17 er fastsat regler for sletning af de pågældende data.

Der må ikke behandles personoplysninger om racemæssig eller etnisk baggrund, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssige tilhørsforhold og personoplysninger om helbredsmæssige og seksuelle forhold, jf. lovens § 11, stk. 1. Efter bestemmelsens stk. 2 gælder dette dog ikke, hvis

1) den pågældende person har givet sit udtrykkelige samtykke til en sådan behandling,

2) behandlingen vedrører personoplysninger, som er blevet offentliggjort af den pågældende person,

3) behandlingen er nødvendig for, at et retskrav kan fastlægges, gøres gældende eller forsvares,

4) behandlingen er nødvendig til beskyttelse af væsentlige hensyn til statens sikkerhed eller rigets forsvar, eller

5) behandlingen vedrører personoplysninger, der er omfattet af kapitel 4 (indgreb i meddelelseshemmeligheden).

Det følger af lovens § 12, stk. 1, at der ikke må behandles personoplysninger om strafbare forhold, væsentlige sociale problemer og andre rent private forhold end de i § 11, stk. 1, nævnte, medmindre det er nødvendigt for varetagelsen af CFCS' opgaver. Efter bestemmelsens stk. 2 må de i stk. 1 nævnte personoplysninger ikke videregives, medmindre

1) den pågældende person har givet sit udtrykkelige samtykke til videregivelsen,

2) videregivelsen sker til varetagelse af private eller offentlige interesser, der klart overstiger hensynet til de interesser, der begrunder hemmeligholdelse, herunder hensynet til den, oplysningen angår,

3) videregivelsen er nødvendig for udførelsen af en myndigheds virksomhed eller påkrævet for en afgørelse, som myndigheden skal træffe,

4) videregivelsen er nødvendig for udførelsen af en persons eller virksomheds opgaver for det offentlige, eller

5) videregivelsen omfatter personoplysninger, der er omfattet af kapitel 4 (indgreb i meddelelseshemmeligheden).

Behandling af personoplysninger skal tilrettelægges således, at der foretages fornøden ajourføring af oplysningerne, jf. lovens § 13. Der skal endvidere foretages den fornødne kontrol for at sikre, at der ikke behandles urigtige eller vildledende personoplysninger. Personoplysninger, der viser sig urigtige eller vildledende, skal snarest muligt slettes eller berigtiges.

Indsamlede personoplysninger må ikke opbevares på en måde, der giver mulighed for at identificere den pågældende person i et længere tidsrum end det, der er nødvendigt af hensyn til de formål, hvortil oplysningerne behandles, jf. lovens § 14. I den forbindelse bemærkes, at der i lovens § 17 er fastsat særlige bestemmelser om sletning af data, der er omfattet af lovens kapitel 4 (indgreb i meddelelseshemmeligheden).

3.3.2 Om sikkerhedsforanstaltninger i forbindelse med behandling af personoplysninger, jf. CFCS-lovens § 18

Ifølge lovens § 18 træffer CFCS passende tekniske og organisatoriske foranstaltninger mod, at oplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, og mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven. For oplysninger, som er af særlig interesse for fremmede magter, skal CFCS træffe foranstaltninger, der muliggør bortskaffelse eller tilintetgørelse i tilfælde af krig eller lignende forhold.

3.4 Analyse og sletning af data omfattet af CFCS-lovens kapitel 4

3.4.1 Om analyse af data, jf. CFCS-lovens § 15

Det følger af lovens § 15, at CFCS kan foretage automatisk analyse af trafikdata, pakkedata og stationære data, der er omfattet af lovens kapitel 4 om indgreb i meddelelseshemmeligheden (§§ 4-6 c). CFCS må alene foretage manuelle analyser af kapitel 4 data i følgende tilfælde:

1) For at opdage, analysere og bidrage til at imødegå sikkerhedshændelser kan trafikdata analyseres i det omfang, det er nødvendigt.

2) Ved begrundet mistanke om en sikkerhedshændelse kan pakkedata og stationære data analyseres i det omfang, det er nødvendigt for at afklare forhold vedrørende hændelsen.

3) Som led i forebyggende sikkerhedstekniske undersøgelser efter § 6 a kan trafikdata, pakkedata og stationære data analyseres i det omfang, det er nødvendigt for at gennemføre undersøgelserne.

4) Som led i det løbende arbejde med at understøtte et højt informationssikkerhedsniveau på Forsvarsministeriets område, herunder ved kontrol af om kommunikation indeholder klassificeret materiale, kan trafikdata og pakkedata, der hidrører fra myndigheder på Forsvarsministeriets område, analyseres.

5) Som led i tekniske test og konfiguration af netsikkerhedstjenestens alarmenheder kan trafikdata og pakkedata analyseres i det omfang, det er nødvendigt for at gennemføre testen. Testen skal afsluttes, så snart formålet med testen er opfyldt. Analysen må alene foretages af medarbejdere, der varetager tekniske drifts- og udviklingsopgaver for CFCS. Øvrige medarbejdere må ikke tilgå oplysninger, der hidrører fra test. Malware, der ved en tilfældighed opdages som led i en teknisk test, må dog analyseres af øvrige medarbejdere i CFCS efter nr. 2.

3.4.2 Om sletning af data, jf. CFCS-lovens § 17

Ifølge lovens § 17, stk. 1, skal data, der behandles efter lovens kapitel 4 om indgreb i meddelelseshemmeligheden (§§ 4-6 c), slettes, når formålet med behandlingen er opfyldt. Bestemmelsen skal ses i sammenhæng med lovens § 14, hvorefter indsamlede personoplysninger generelt ikke må opbevares på en måde, der giver mulighed for at identificere den pågældende person i et længere tidsrum end det, der er nødvendigt af hensyn til de formål, hvortil oplysningerne behandles. Mens lovens § 14 finder anvendelse på al behandling af alle personoplysninger i CFCS, finder de særlige regler i lovens § 17 alene anvendelse på de data, der behandles på baggrund af indgreb i meddelelseshemmeligheden.

Ifølge lovforslagets bemærkninger til § 17 vil der på baggrund af bestemmelsen ske en løbende vurdering af de behandlede data med henblik på at sikre, at data, der ikke længere er relevante i forhold til netsikkerhedstjenestens formål og aktiviteter, straks slettes.

Herudover fremgår det af lovens § 17, stk. 2, at uanset at formålet med behandlingen ikke er opfyldt, jf. stk. 1, må

1) data, der knytter sig til en sikkerhedshændelse, højst opbevares i fem år,

2) data, der ikke knytter sig til en sikkerhedshændelse, men som strammer fra myndigheder, som i særlig grad beskæftiger sig med udenrigs-, sikkerheds- og forsvarspolitiske forhold, samt virksomheder og organisationer, hvis aktiviteter har særlig betydning for disse forhold, højst opbevares i tre år, og

3) data, der ikke knytter sig til en sikkerhedshændelse, højst opbevares i 13 måneder.

Bestemmelsen fastsætter øvre grænser for, hvor længe data, der ikke er slettet efter lovens § 17, stk. 1, kan opbevares, og bestemmelsen finder dermed anvendelse på data, hvor det er blevet vurderet, at der fortsat er behov for behandling i netsikkerhedstjenesten. Uanset at formålet med behandlingen således i disse tilfælde endnu ikke er opfyldt, vil data skulle slettes inden for de absolutte frister, som er fastsat i bestemmelsen. Såfremt data, der knytter sig til en sikkerhedshændelse, inden for den femårige periode igen konstateres anvendt i forbindelse med en sikkerhedshændelse, vil en ny femårig periode begynde. Fristerne i stk. 2 regnes fra tidspunktet for CFCS' registrering af de pågældende data, jf. stk. 3.

Forsvarsministeren har i 2021 – på baggrund af tilsynets kontrol – foretaget en vurdering af betydningen af CFCS-lovens § 17, stk. 1, for CFCS' forpligtelse til at slette data indhentet via centrets sensornetværk. Forsvarsministeren vurderer, at sensordata, som CFCS på baggrund af en analyse har vurderet ikke knytter sig til en sikkerhedshændelse, ikke skal slettes i henhold til CFCS-lovens § 17, stk. 1.

Dette skyldes, at CFCS skal have mulighed for at søge i historiske data, når centret får ny viden eller værktøjer. Formålet med behandlingen af sensordata kan derfor ikke siges

at være opfyldt i henhold til CFCS-lovens § 17, stk. 1, men slettes alene efter de absolutte slettefrister i CFCS-lovens § 17, stk. 2.

Selv i tilfælde, hvor det endegyldigt kan konkluderes, at der er tale om godartede data, der ikke senere vil kunne vise sig at være knyttet til et cyberangreb, vil sensordata skulle opbevares i den fulde periode, som fremgår af CFCS-lovens § 17, stk. 2, idet sletning af denne type data potentielt vil kunne forringe CFCS' muligheder for at tegne et normalbillede af internetaktiviteten hos den pågældende organisation.

Forsvarsministeren vurderer derimod, at sensordata, som CFCS har vurderet at knytte sig til en sikkerhedshændelse, skal slettes i henhold til CFCS-lovens § 17, stk. 1, i det omfang centret måtte vurdere, at de konkrete data ikke vil være relevante for CFCS' fremtidige muligheder for at opdage, analysere og bidrage til at imødegå cyberangreb. Forsvarsministeren fremhæver i den forbindelse, at CFCS er tillagt en betydelig grad af skøn i forhold til, hvornår formålet med behandlingen i disse tilfælde er opfyldt.

Lovens § 17, stk. 1 og 2, finder ikke anvendelse på data, der er videregivet til andre end den myndighed eller virksomhed, som data hidrører fra, jf. lovens § 17, stk. 5.

Personoplysninger i data, som CFCS får adgang til som led i forebyggende sikkerhedstekniske undersøgelser efter § 6 a, skal ifølge lovens § 17, stk. 6, slettes eller anonymiseres, når den sikkerhedstekniske undersøgelse er afsluttet. Konstaterer CFCS, at der i de pågældende data er indeholdt følsomme personoplysninger, skal disse slettes uden unødigt ophold.

I helt særlige tilfælde kan de ovenfor beskrevne slettefrister kortvarigt suspenderes, hvis væsentlige hensyn til varetagelsen af CFCS' opgaver gør det nødvendigt, jf. § 17, stk. 7. CFCS skal straks underrette tilsynet om suspensionen og baggrunden herfor.

Ifølge lovens § 17 a finder bestemmelserne i lovens § 17 ikke anvendelse på data, der er deponeret på fiktive angrebsmål efter § 6 b eller modtaget via infrastruktur omfattet af § 6 c, såfremt CFCS ikke udtager disse data til nærmere vurdering. Disse data slettes i stedet hurtigst muligt.

3.5 Videregivelse og udveksling af oplysninger omfattet af CFCS-lovens kapitel 4

3.5.1 Om videregivelse, jf. CFCS-lovens § 16

Efter lovens § 16 kan CFCS i en række nærmere definerede tilfælde videregive data, der er omfattet af lovens kapitel 4 om indgreb i meddelelseshemmeligheden (§§ 4-6 c). Kravene til videregivelsen afhænger både af, hvem der er tiltænkt som modtager af data, samt af hvilken type af data der videregives.

CFCS kan ifølge lovens § 16, stk. 1, videregive trafikdata, der er omfattet af kapitel 4, til:

1) Politiet, såfremt der er begrundet mistanke om en sikkerhedshændelse.

2) Den tilsluttede myndighed eller virksomhed, hvorfra de pågældende data hidrører,

såfremt der er begrundet mistanke om en sikkerhedshændelse, og hvis det er nødvendigt for udførelsen af CFCS' opgaver.

3) Danske myndigheder, udbydere af offentlige elektroniske kommunikationsnet og -tjenester og andre netsikkerhedstjenester samt myndigheder og virksomheder i øvrigt i forbindelse med CFCS' udsendelse af sikkerhedsvarslinger, såfremt der er begrundet mistanke om en sikkerhedshændelse, og såfremt det er nødvendigt for udførelsen af centrets opgaver.

CFCS kan ifølge lovens § 16, stk. 2, videregive pakkedata, der er omfattet af kapitel 4, til:

1) Politiet, såfremt der er begrundet mistanke om en sikkerhedshændelse.

2) Den tilsluttede myndighed eller virksomhed, hvorfra de pågældende data hidrører, såfremt der er begrundet mistanke om en sikkerhedshændelse.

CFCS kan ifølge lovens § 16, stk. 3, videregive stationære data, der er omfattet af kapitel 4, til:

1) Politiet, såfremt der er begrundet mistanke om en sikkerhedshændelse.

2) Den myndighed, virksomhed eller borger, hvorfra de pågældende data hidrører, såfremt der er begrundet mistanke om en sikkerhedshændelse.

3) Andre netsikkerhedstjenester, såfremt CFCS har modtaget de pågældende data i medfør af § 6 b eller § 6 c.

CFCS kan ifølge lovens § 16, stk. 4, videregive malware, der er omfattet af kapitel 4, til:

1) Politiet.

2) Den myndighed eller virksomhed, hvorfra de pågældende data hidrører.

3) Danske myndigheder, udbydere af offentlige elektroniske kommunikationsnet og -tjenester og andre netsikkerhedstjenester samt myndigheder og virksomheder i øvrigt i forbindelse med CFCS' udsendelse af sikkerhedsvarslinger.

CFCS kan ifølge lovens § 16, stk. 5, alene videregive data, som stammer fra tekniske test og konfiguration af netsikkerhedstjenestens alarmenheder i følgende tilfælde:

1) Malware, der er opdaget ved en tilfældighed, kan videregives til politiet, til den myndighed eller virksomhed, hvorfra de pågældende data hidrører, til danske myndigheder, til udbydere af offentlige elektroniske kommunikationsnet og -tjenester og til andre netsikkerhedstjenester samt til myndigheder og virksomheder i øvrigt i forbindelse med CFCS' udsendelse af sikkerhedsvarslinger.

2) Trafikdata kan videregives til den tilsluttede myndighed eller virksomhed, hvorfra de pågældende data hidrører.

CFCS må ifølge lovens § 16, stk. 6, i forbindelse med forebyggende sikkerhedstekniske undersøgelser efter § 6 a alene videregive oplysninger vedrørende myndighedens eller virksomhedens medarbejdere, hvis det sker i anonymiseret form.

3.5.2 Om udveksling af data med FE, jf. CFCS-cirkulærets § 2

I de almindelige bemærkninger til CFCS-loven anføres om den interne udveksling af data i FE, at denne i overensstemmelse med almindelige forvaltningsretlige principper ikke er lovreguleret.

Dette indebærer, at der som udgangspunkt er fri adgang til at udveksle data internt i FE, herunder mellem CFCS og den øvrige del af efterretningstjenesten, hvis dette er nødvendigt for at løse myndighedens opgaver, og der i øvrigt er tale om et sagligt formål. Det sikrer, at alle de relevante ressourcer i FE hurtigt og effektivt kan indsættes ved den meget store andel af cyberangreb mod Danmark, som hidrører fra udlandet, og hvor FE som udenrigs-efterretningstjeneste kan bidrage med en række værdifulde oplysninger.

I overensstemmelse hermed er det i § 2, stk. 1, i CFCS-cirkulæret fastsat, at CFCS kun må udveksle data, der er omfattet af lovens kapitel 4, med den øvrige del af FE, når

1) udvekslingen er nødvendig for at understøtte et højt informationssikkerhedsniveau,

2) udvekslingen sker med udtrykkeligt angivne og saglige formål, og

3) der er begrundet mistanke om en sikkerhedshændelse.

Efter bestemmelsens stk. 2 finder stk. 1, nr. 3, ikke anvendelse på data, der hidrører fra myndigheder på Forsvarsministeriets område.

Det følger af bestemmelsens stk. 3, at enhver udveksling af data skal registreres af CFCS.

Årsredegørelse 2021
Center for Cybersikkerhed
Udgivet af Tilsynet med Efterretningstjenesterne, maj 2022

Layout + illustrationer: Eckardt ApS
Portrætfotos: Lars Engelgaar / Sophie Kalckar

Publikationen kan downloades fra tilsynets hjemmeside på www.tet.dk

Medlemmer af Tilsynet med Efterretningstjenesterne

Landsdommer Michael Kistrup, Østre Landsret (formand)
Juridisk chef Pernille Christensen, Kommunernes Landsforening
Professor Henrik Udsen, Københavns Universitet
Professor Rebecca Adler-Nissen, Københavns Universitet
Koncerndirektør David Hellemann, Nykredit (udtrådt pr. 1. februar 2022)

Tilsynet med Efterretningstjenesterne
Borgergade 28, 1. sal, 1300 København K
www.tet.dk