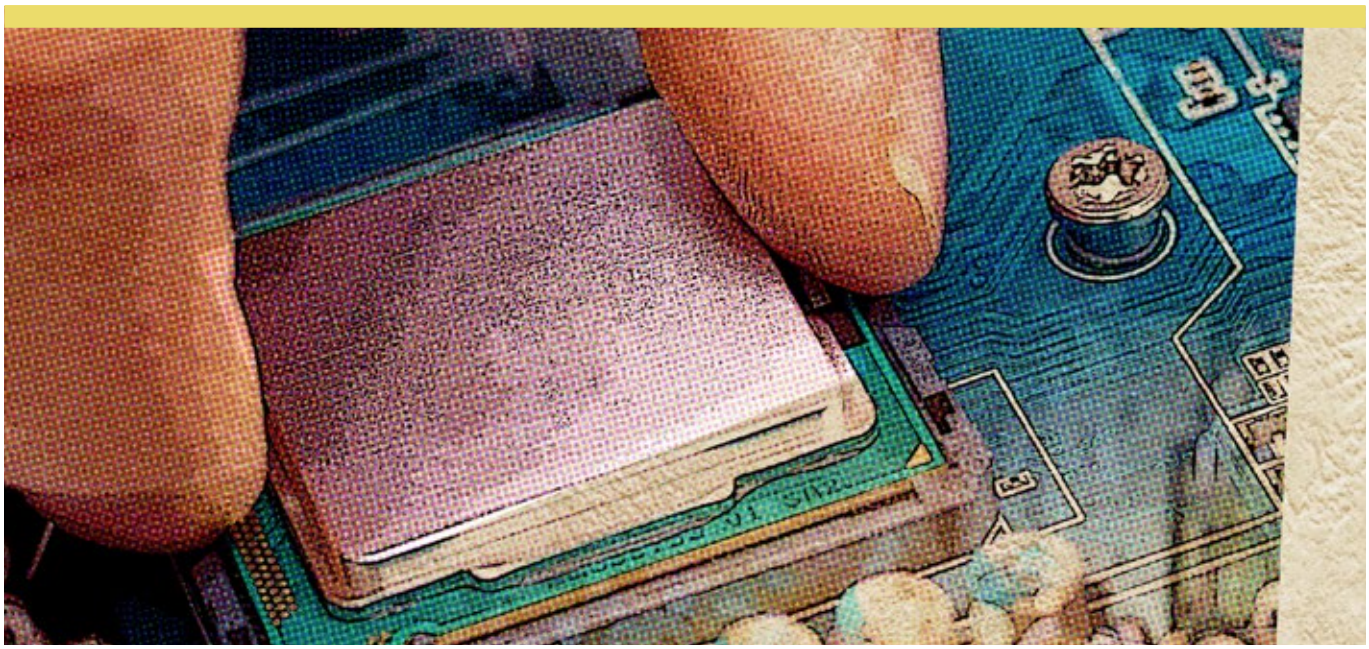
Tilsynet med Efterretningstjenesterne



Årsredegørelse 2019

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 2019. Redegørelsen skal offentliggøres.

København, august 2020

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.

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. For 2019 fremhæves følgende centrale og principielle dele af redegørelsen:

- **Tilsynets** kontrol af CFCS i 2019 viste, at centret generelt overholder CFCS-lovgivningens bestemmelser om indgreb i meddelelseshemmeligheden, om behandling af personoplysninger samt om analyse og videregivelse.

- **Tilsynet** har imidlertid på baggrund af sin kontrol af CFCS' anvendelse af centrets sensornetværk, jf. afsnit 1.2.1, konstateret, at centrets behandling af sensordata i 67 procent af de udtrukne tilfælde ikke var i overensstemmelse med lovgivningens krav om løbende sletning, jf. CFCS-lovens § 17, stk. 1, idet tilsynet fandt, at det af centret oplyste formål ikke var tilstrækkeligt grundlag for behandlingen.

- **Tilsynet** har endvidere på baggrund af sin kontrol af arbejdsstationer i CFCS, jf. afsnit 1.2.4, konstateret, at centrets behandling af personoplysninger i ét tilfælde ikke var i overensstemmelse med CFCS-loven, idet tilsynet fandt, at det af centret oplyste formål ikke var tilstrækkeligt grundlag for behandlingen. Tilsynet finder det kritisabelt, at centrets første høringssvar i forbindelse med kontrollen indeholdt fejlagtige oplysninger om centrets behandling af oplysningerne, hvilket centret imidlertid berigtigede i et supplerende høringssvar, samt at centret havde en lang sagsbehandlingstid i forbindelse med tilsynets supplerende høring i sagen. Tilsynet finder det imidlertid positivt, at CFCS' på baggrund af kontrollen har besluttet at udarbejde nye retningslinjer på området.

Det bemærkes, at ovenstående henvisninger imidlertid alene udgør et mindre udsnit af tilsynets kontrol af CFCS i 2019, hvor tilsynet har haft særlige eller principielle bemærkninger. For det fulde billede af tilsynets kontrol af CFCS skal redegørelsen læses i sin helhed.

Forord

Tilsynet med Efterretningstjenesterne er et særligt uafhængigt kontrolorgan, der blandt andet fører tilsyn med, at Center for Cybersikkerhed (CFCS) behandler oplysninger om fysiske personer i overensstemmelse med lovgivningen. Tilsynet blev oprettet ved lov om Politiets Efterretningstjeneste (PET), der trådte i kraft den 1. januar 2014.

Sigtet med nærværende redegørelse er at informere om karakteren af det tilsyn, der udøves vedrørende CFCS. Redegørelsen indeholder oplysninger om de forhold, som tilsynet i 2019 har valgt særligt at interessere sig for, og om i hvor mange tilfælde tilsynet har fundet, at centrets behandling af personoplysninger ikke har været i overensstemmelse med reglerne.

Som i de forgangne år har tilsynet i 2019 haft fokus på at konsolidere og styrke grundlaget for tilsynets kontrol af henholdsvis CFCS, Forsvarets Efterretningstjeneste (FE) og PET, herunder ved løbende udvikling af tilsynets risiko- og væsentlighedsvurdering af tjenesterne og centret samt de standarder og metoder, som anvendes i den retlige kontrol heraf. Det er afgørende for tilsynet, at de enkelte kontroller er velunderbyggede og -dokumenterede, og at de er tilrettelagt på baggrund af en tilstrækkelig efterretningsfaglig og teknisk forståelse. Tilsynet har i 2019 endvidere igangsat flere udviklingsprojekter med henblik på at sikre en mere effektiv systemunderstøttelse af tilsynets kontrolvirksomhed.

Tilsynet har i 2019 gennemført omfattende og intensive kontroller med CFCS' behandling af oplysninger om fysiske personer. Som i de foregående år har tilsynet prioriteret kontroller med fokus på CFCS' overholdelse af reglerne om analyse, videregivelse og sletning af data tilvejebragt ved indgreb i meddelelseshemmeligheden samt centrets behandling af personoplysninger i øvrigt.

Tilsynet har i 2019 fortsat sit samarbejde med hollandske Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD), belgiske Comité permanent de contrôle de services de renseignements et de sécurité (Committee I), norske Stortingets Kontrollutvalg for etterretnings-, overvåknings- og sikkerhetstjeneste (EOS-utvalget) og schweiziske Unabhängige Aufsichtsbehörde über die nachrichtendienstlichen Tätigkeiten (AB-ND). Samarbejdet blev i 2019 udbygget med det britiske Investigatory Powers Commissioner's Office (IPCO). Fokus i dette samarbejde er erfaringsudveksling omkring kontrolmetoder samt drøftelse af juridiske emner af fælles relevans. Samarbejdet har blandt andet resulteret i, at tilsynet i juni 2019 afholdt konference i København, hvor emnet var drøftelse af fælles standarder for kontrol af efterretningstjenester.

Tilsynet har i november 2019 endvidere deltaget i et nordisk møde i Oslo med tilsynsmyndigheder fra Norge, Sverige og Finland.

Foruden tilsynets tætte samarbejde med udvalgte tilsynsmyndigheder deltog tilsynet i december 2019 i en fælles europæisk konference for tilsynsmyndigheder i Haag, hvor 18 europæiske lande deltog.

I efteråret 2019 har tilsynet desuden fået et nyt medlem.

Endelig trådte lov nr. 555 af 7. maj 2019 om ændring af lov om Center for Cybersikkerhed (Initiativer til styrkelse af cybersikkerheden) i kraft den 1. juli 2019, hvorved blandt andet reglerne om CFCS' videregivelse af oplysninger blev ændret.

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 med CFCS med henblik på, at kontrollen får den størst mulige effekt inden for de rammer, som er sat for tilsynets virke.

Tilsynets kontrolarbejde består af tre delelementer: planlægning, udførsel og verificering. Tilsynet evaluerer derudover løbende på sit arbejde med alle tre elementer.

Tilsynets planlægning af kontrollerne for det kommende år sker på baggrund af en årlig risikovurdering vedrørende processer og systemer hos CFCS. Formålet med risikovurderingen er at vurdere risici for lovbrud i relation til indgreb i meddelelseshemmeligheden, behandling, analyse, videregivelse og sletning af oplysninger om den persongruppe, der er omfattet af tilsynets kompetence. På baggrund heraf udarbejder tilsynet en risikoanalyse, som danner grundlag for udvælgelsen af det kommende års kontroller.

Formålet med risikoanalysen 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 politisk side er tillagt særlig vægt. Områder, hvor der vurderes at være en lav risiko for fejl, kontrolleres som hovedregel én gang hvert tredje år med henblik på at skabe fuldstændighed i kontrol af CFCS og sikre, at vurderingen af risiko for fejl på området fortsat er retvisende. Endvidere foretager tilsynet inspektioner af systemer, der i forbindelse med risikovurderingen er vurderet som værende ikke relevante for tilsynets kontrol, med henblik på at efterprøve om relevansvurderingen er korrekt.

Planlægningen af tilsynets kontrol for det kommende år afsluttes ved udgangen af det foregående år, med henblik på at erfaringerne fra dette års kontrol kan indgå som en del af tilsynets risikovurdering og -analyse.

Selve kontrollen gennemføres løbende hen over året. Kontrollen af de enkelte områder gennemføres som udgangspunkt af tilsynets sekretariat. Efter en konkret vurdering anmodes CFCS om uddybende bemærkninger. Sekretariatet forelægger på dette grundlag resultaterne af kontrollen for tilsynet, som beslutter, om kontrollerne er tilstrækkelig belyst, eller om der er behov for at indhente yderligere oplysninger eller foretage nærmere drøftelser med CFCS.

Tilsynet benytter sig af en række forskellige metoder i kontrollen af de enkelte områder, heriblandt fuldstændig kontrol, simpelt tilfældige eller stratificerede stikprøver, indholdsscreening og

interviewbaseret kontrol. Tilsynets valg af metode sker på baggrund risikoanalysen af området, erfaringer fra tidligere kontroller og de faktiske forhold, som tilsynet konstaterer i forbindelse med kontrollen. Endvidere afholder tilsynet forud for kontrol af ikke tidligere kontrollerede områder 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.

Tilsynets direkte adgang til CFCS' systemer sikrer, at centret ikke kan forudse, hvilke oplysninger og sager, der bliver genstand for tilsynets kontrol. I nogle tilfælde er det dog 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 hos centret. Åbenheden giver endvidere CFCS mulighed for at tage højde for tilsynets kontrol i tilrettelæggelsen af den 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.

Tilsynet foretager verificering ved løbende kortlægning af CFCS' systemlandskab på server-, komponent- og applikationsniveau med henblik på at kunne foretage en fuldstændig risikovurdering af samtlige processer og systemer i centret. Tilsynet afsætter hvert år væsentlige ressourcer til verificering af de oplysninger, som modtages fra CFCS vedrørende centrets systemlandskab. Formålet med verificeringen er at sikre, at tilsynets kontrol beror på oplysninger fra CFCS, hvis rigtighed tilsynet har efterprøvet.

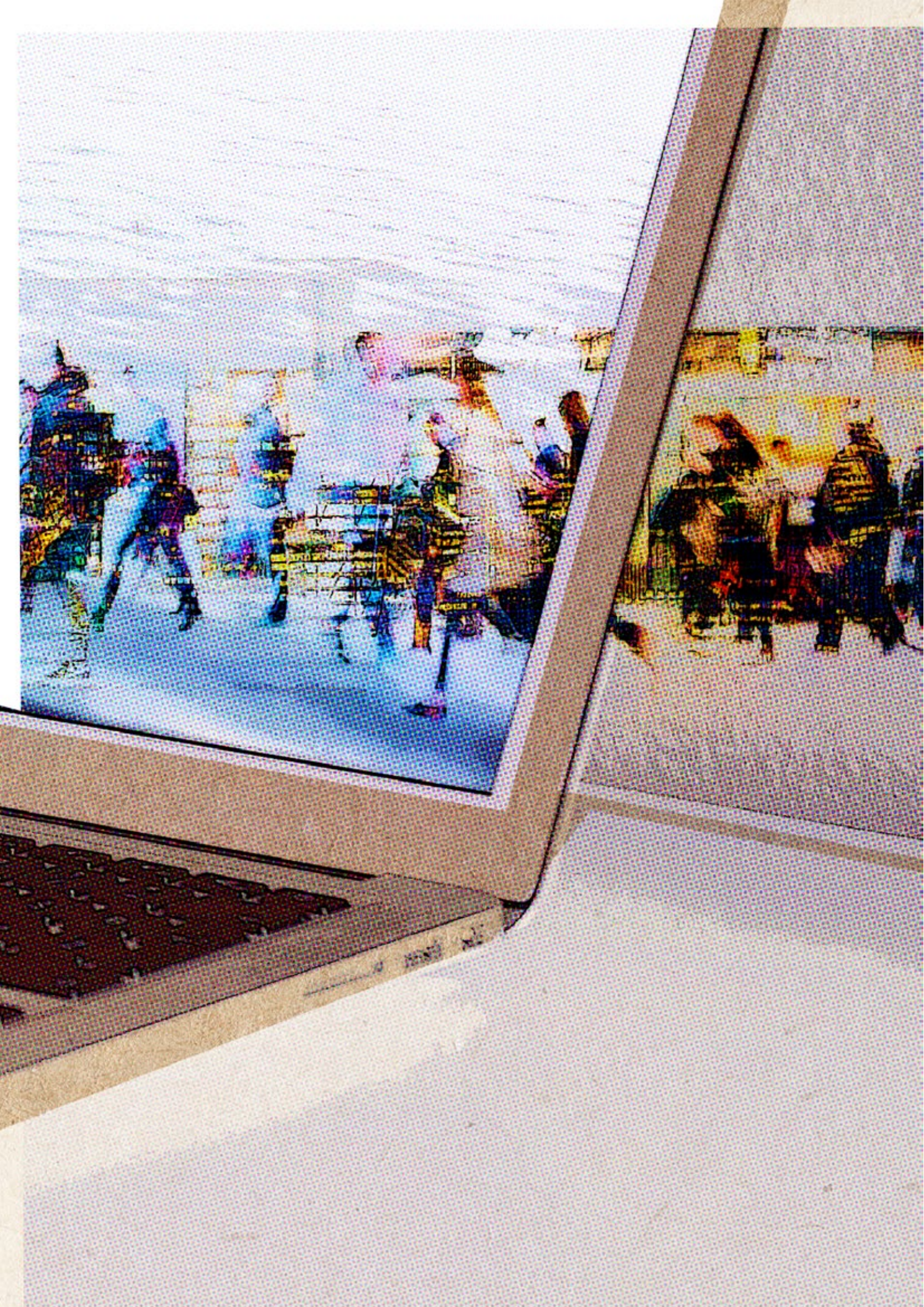
1.2 Kontrol af CFCS i 2019

Med henblik på at kontrollere at CFCS i forbindelse med behandling af oplysninger om fysiske personer overholder reglerne i CFCS-loven, har tilsynet i 2019 foretaget kontrol af centrets

- anvendelse af centrets sensornetværk (1.2.1),
- behandling af oplysninger i relation til indleverede medier (1.2.2),
- drev (1.2.3),
- arbejdsstationer (1.2.4),
- videregivelse af oplysninger til andre myndigheder, virksomheder og samarbejdspartnere (1.2.5),
- udveksling af oplysninger med den øvrige del af FE (1.2.6) og
- interne kontrol (1.2.7).

Sammenfatning af tilsynets kontroller i 2019

Tilsynets kontrol af CFCS' sensornetværk viste, jf. afsnit 1.2.1, at centret har iagttaget lovgivningens krav vedrørende tilvejebringelse af oplysninger. Tilsynet har imidlertid konstateret, at CFCS' behandling af data hentet fra centrets sensornetværk i 67 procent af de udtrukne tilfælde ikke



var i overensstemmelse med lovgivningens krav, jf. CFCS-lovens § 17, stk. 1, hvoraf det følger, at data, der behandles efter lovens kapitel 4 om indgreb i meddelelseshemmeligheden (§§ 4-6), skal slettes, når formålet med behandlingen er opfyldt, idet tilsynet fandt, at det af centret oplyste formål ikke var tilstrækkeligt grundlag for behandlingen.

Tilsynets kontrol af CFCS' behandling af oplysninger i relation til indleverede medier viste, jf. afsnit 1.2.2, at centret i otte tilfælde ikke overholdt lovgivningens krav til sikkerhedsforanstaltninger i forbindelse med behandling af oplysninger, jf. CFCS-lovens § 18, stk. 1, men at centrets håndtering af eksterne medier i øvrigt var tilrettelagt i overensstemmelse med lovgivningens krav.

Tilsynets kontrol af arbejdsstationer viste, jf. afsnit 1.2.4, at CFCS' medarbejdere generelt var opmærksomme på, at behandling af oplysninger skal ske i overensstemmelse med loven og centrets interne retningslinjer, men at CFCS i ét tilfælde behandlede oplysninger i strid med CFCS-loven, idet tilsynet fandt, at det af centret oplyste formål ikke var tilstrækkeligt grundlag for behandlingen. Tilsynet finder det kritisabelt, at CFCS' første høringssvar i forbindelse med kontrollen indeholdt fejlagtige oplysninger om centrets behandling af oplysningerne, hvilket centret imidlertid berigtigede i et supplerende høringssvar, samt at centret havde en lang sagsbehandlingstid i forbindelse med tilsynets supplerede høring i sagen. Tilsynet finder det imidlertid positivt, at CFCS på baggrund af kontrollen har besluttet at udarbejde nye retningslinjer på området.

Tilsynets øvrige kontroller af CFCS' behandling, videregivelse samt udveksling af oplysninger viste, jf. afsnit 1.2.3, 1.2.5 og 1.2.6, at centret har iagttaget lovgivningens krav til behandling, videregivelse og udveksling af oplysninger.

Endvidere viste kontrollen af CFCS' interne kontrol, jf. afsnit 1.2.7, at centret generelt har tilrettelagt og gennemført sin interne kontrol tilfredsstillende.

1.2.1 Kontrol af CFCS' anvendelse af centrets 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, der 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.

Tilsynet har i 2019 foretaget en kontrol af CFCS' tilvejebringelse af oplysninger fra centrets sensornetværk på baggrund af alarmer samt den efterfølgende behandling, herunder sletning, af hentet sensordata.

Tilsynet foretog en stikprøve af et antal tilfældigt udvalgte hentninger fra sensornetværket med henblik på at kontrollere, om oplysningerne efterfølgende blev slettet i overensstemmelse med CFCS-lovens § 17, stk. 1, hvoraf det følger, at data, der behandles efter lovens kapitel 4 om indgreb i meddelelseshemmeligheden (§§ 4-6), skal slettes, når formålet med behandlingen er opfyldt.

! **Tilsynets bemærkninger**

Tilsynets kontrol af CFCS' anvendelse af centrets sensornetværk viste, at centret har iagttaget lovgivningens krav vedrørende tilvejebringelse af oplysninger.

Tilsynet har imidlertid på baggrund af kontrollen konstateret, at CFCS' behandling af sensordata i 67 procent af de udtrukne tilfælde ikke var i overensstemmelse med lovgivningens krav om løbende sletning, jf. CFCS-lovens § 17, stk. 1, idet tilsynet fandt, at det af centret oplyste formål ikke var tilstrækkeligt grundlag for behandlingen.

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 2019 foretaget en kontrol af CFCS' behandling af oplysninger i relation til indleverede medier.

Tilsynet foretog et inspektionsbesøg i CFCS, hvor alle indleverede medier blev kontrolleret.

! **Tilsynets bemærkninger**

Tilsynets kontrol af CFCS' behandling af oplysninger i relation til indleverede medier viste, at centret i otte tilfælde ikke overholdt lovgivningens krav til sikkerhedsforanstaltninger i forbindelse med behandling af oplysninger, jf. CFCS-lovens § 18, stk. 1, men at centrets håndtering af eksterne medier i øvrigt var tilrettelagt i overensstemmelse med lovgivningens krav.

1.2.3 Kontrol af drev i CFCS

CFCS anvender drev til opbevaring af oplysninger, som anvendes i centrets afdelinger og sektioner, men som ikke nødvendigvis registreres i centrets centrale systemer.

Tilsynet har i 2019 foretaget kontrol af CFCS' behandling af oplysninger på drev.

Tilsynet foretog kontrol af drev, som anvendes af medarbejdere tilknyttet én afdeling og tre sektioner i CFCS. Kontrollen blev gennemført ved indholdsscreeninger og stikprøvekontroller.

! **Tilsynets bemærkninger**

Tilsynets kontrol af CFCS' behandling af oplysninger på drev viste, at centret har iagttaget lovgivningens bestemmelser herom.

1.2.4 Kontrol af arbejdsstationer i CFCS

Tilsynet har i 2019 foretaget kontrol af et antal medarbejderes arbejdsstationer.

Tilsynets foretog kontrol af et antal tilfældigt udvalgte arbejdsstationer, herunder af personlige drev, mailsystemer, eksterne lagringsenheder og fysiske dokumenter. I forbindelse med den stikprøvevise gennemgang af oplysningerne på den enkelte arbejdsstation stillede tilsynet spørgsmål til vedkommende medarbejder om pågældendes kendskab til reglerne om behandling, herunder sletning, af oplysninger vedrørende fysiske personer.

! Tilsynets bemærkninger

Tilsynets kontrol af udvalgte arbejdsstationer viste, at CFCS' medarbejdere generelt overholdt CFCS-loven og centrets interne retningslinjers regler om behandling af oplysninger. Kontrollen viste endvidere, at medarbejderne generelt var opmærksomme på, at behandling af oplysninger sker i overensstemmelse med CFCS-lovgivningen og centrets interne retningslinjer.

Tilsynets kontrol af udvalgte arbejdsstationer viste imidlertid, at en medarbejder i ét tilfælde behandlede oplysninger i strid med CFCS-loven, idet tilsynet fandt, at det af centret oplyste formål ikke var tilstrækkeligt grundlag for behandlingen.

I forbindelse med kontrollen foretog tilsynet supplerende høring af CFCS, idet centrets indledende høringssvar gav anledning til spørgsmål. CFCS berigtigede i sit supplerende høringssvar fejlagtige oplysninger vedrørende behandlingen, som havde været indeholdt i centrets indledende høringssvar. Tilsynet modtog først centrets supplerende høringssvar fem måneder efter fremsendelsen af den supplerende høring. Tilsynet finder det kritisabelt, at CFCS afgav fejlagtige oplysninger til tilsynet, samt at centret havde en lang sagsbehandlingstid i forbindelse med tilsynets supplerede høring.

Tilsynet finder det imidlertid positivt, at CFCS' på baggrund af kontrollen har besluttet at udarbejde nye retningslinjer vedrørende medarbejderes behandling af oplysninger om fysiske personer.

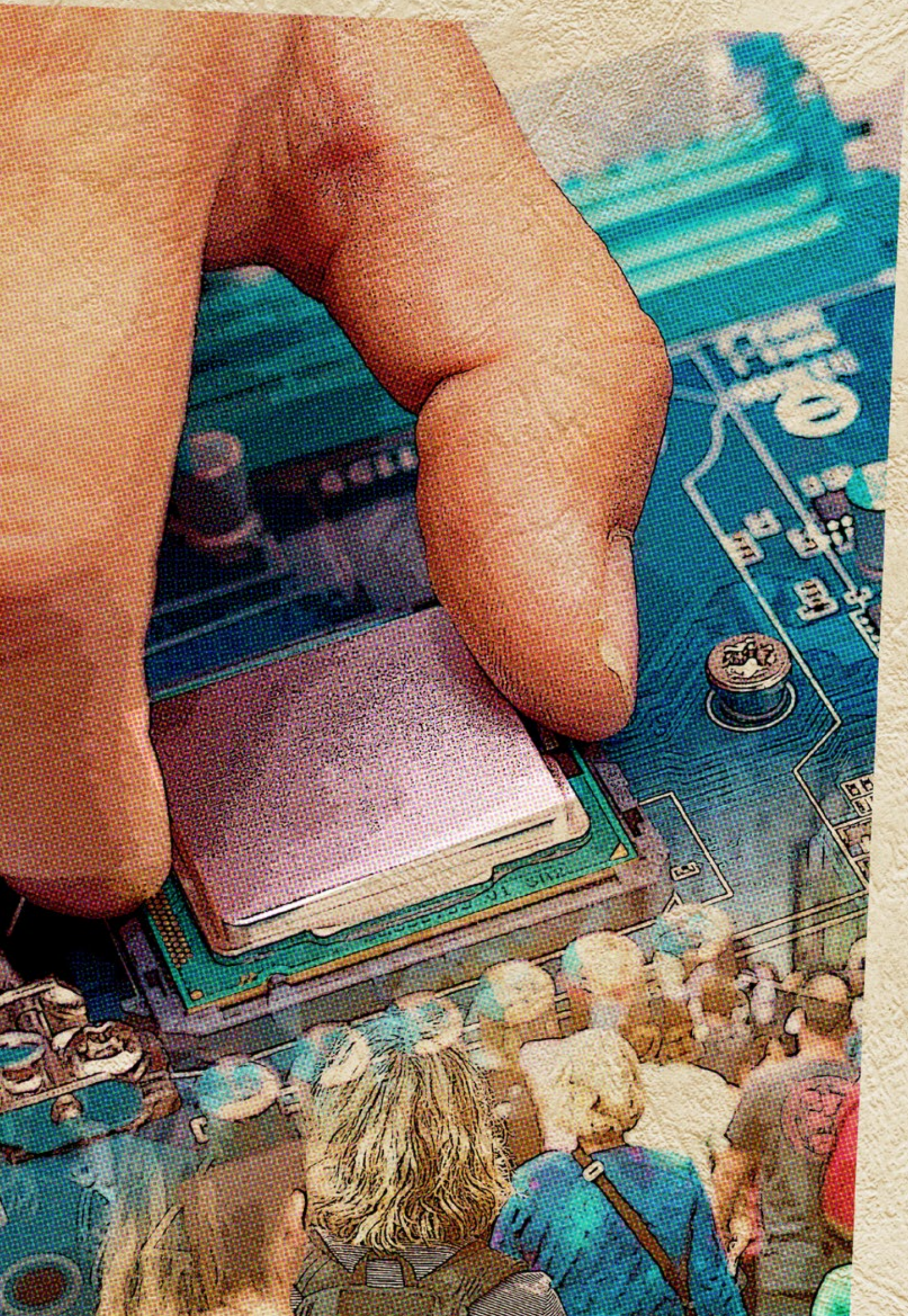
1.2.5 Kontrol af CFCS' videregivelse af oplysninger til andre myndigheder, virksomheder og samarbejdspartnere

Tilsynet har i 2019 foretaget kontrol af CFCS' videregivelse af data indeholdende personoplysninger til andre myndigheder, virksomheder og udenlandske samarbejdspartnere med fokus på centrets overholdelse af CFCS-lovens §§ 10 og 16.

Tilsynet trak en stikprøve på et antal tilfældigt udvalgte videregivelser.

! Tilsynets bemærkninger

Tilsynets kontrol af CFCS' videregivelse af data indeholdende personoplysninger til andre myndigheder, virksomheder og samarbejdspartnere viste, at centret har iagttaget lovgivningens bestemmelser herom.



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

Tilsynet har i 2019 foretaget kontrol af CFCS' udveksling af data indeholdende personoplysninger, der stammer fra indgreb i meddelelseshemmeligheden, 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 trak en stikprøve på et antal udvalgte udvekslinger fra CFCS med 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 viste, at centret har iagttaget CFCS-cirkulærets bestemmelser herom.

1.2.7 Kontrol af CFCS' interne kontrol

Tilsynet har ved sin kontrol af CFCS i 2019 foretaget kontrol af centrets interne kontrol. Kontrollen har omfattet CFCS' interne kontrol samt centrets planlægning heraf for 2020 og er foretaget ved gennemgang af udleveret dokumentation og drøftelser med centret.

! **Tilsynets bemærkninger**
Tilsynets kontrol af CFCS' interne kontrol i 2019 viste, at centret generelt har tilrettelagt og gennemført den interne kontrol tilfredsstillende.

2

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 2019:

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, der påvirker dansk kritisk infrastruktur, herunder de seks samfundskritiske sektorer i Danmark.

I 2019 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 også 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.

3 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 centret 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 2019:

Tabel 1 Modtagne klagesager over CFCS' behandling af personoplysninger

Kategorier	2019
Klagesager modtaget i CFCS	0
Klagesager modtaget i tilsynet	0

Tabel 2 Aktindsigtssager

Kategorier	2019
Fuld aktindsigt	0
Delvis aktindsigt	2
Afslag på aktindsigt	3
Ingen dokumenter lokaliseret til at give eller afslå aktindsigt i	1
Total	**6**

Tabel 3 Sikkerhedshændelser* efter alvorlighedsgrad

Kategorier	2019
Alvorlige cyberangreb	1
Større cyberangreb	2
Moderate cyberangreb	30
Mindre cyberangreb	383
Ingen/begrænset effekt**	746
Total	**1.162**

* Sikkerhedshændelser defineres i overensstemmelse med § 2, nr. 1, i lov om Center for Cybersikkerhed.
** Kategorien "Ingen/begrænset effekt" inkluderer falske positiver.

Tabel 4 CFCS' videregivelser og udvekslinger af oplysninger*

Kategorier	2019
Videregivelser	108
Udvekslinger	31

* 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 1.2.5.

4

Presseomtale i 2019

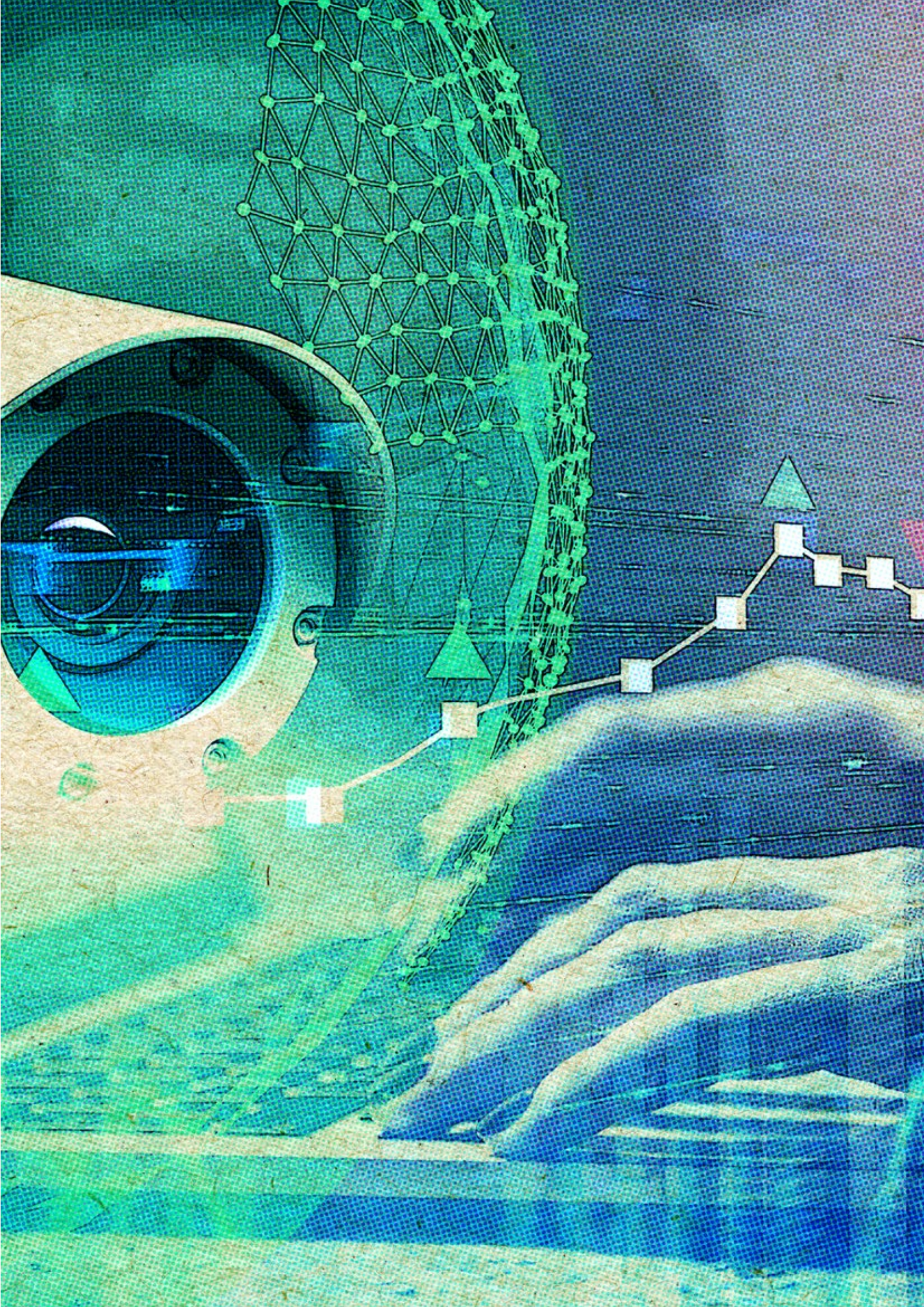
CFCS' virksomhed, samt de rammer som Folketinget og regeringen sætter for denne, heriblandt tilsynets kontrol, er løbende genstand for omtale i de danske medier.

Tilsynet ønsker i videst muligt omfang at bidrage til, at pressen og dermed offentligheden får den bedst mulige indsigt i tilsynets kontrol af CFCS, under hensyntagen til det behov for hemmeligholdelse som følger af centrets særlige funktion.

Tilsynet følger løbende med i den offentlige debat om tilsynets kontrol af CFCS, med henblik på at vurdere om tilsynet kan bidrage til en bedre forståelse af tilsynets rolle og kontrolmuligheder samt resultaterne af tilsynets kontrol.

Tilsynets betydning som kontrolorgan er blandt andet blevet fremhævet i den offentlige debat, der opstod på baggrund af ændringen af CFCS-loven i maj 2019.

Endvidere udgav tænketanken "Stiftung Neue Verantvorden" i november 2019 rapporten "Data-driven intelligence Oversight - Recommendations for a System Update", hvori tilsynets arbejdsmetoder blev fremhævet. Rapporten foreslår syv redskaber til reformering af tilsyn med efterretningstjenester på tværs af Europa og fremhæver i den forbindelse det danske tilsyns risikobaserede arbejde som eksempel på, hvordan udfordringer med effektiv allokering af knappe ressourcer til kontrol af efterretningstjenester kan håndteres.



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.

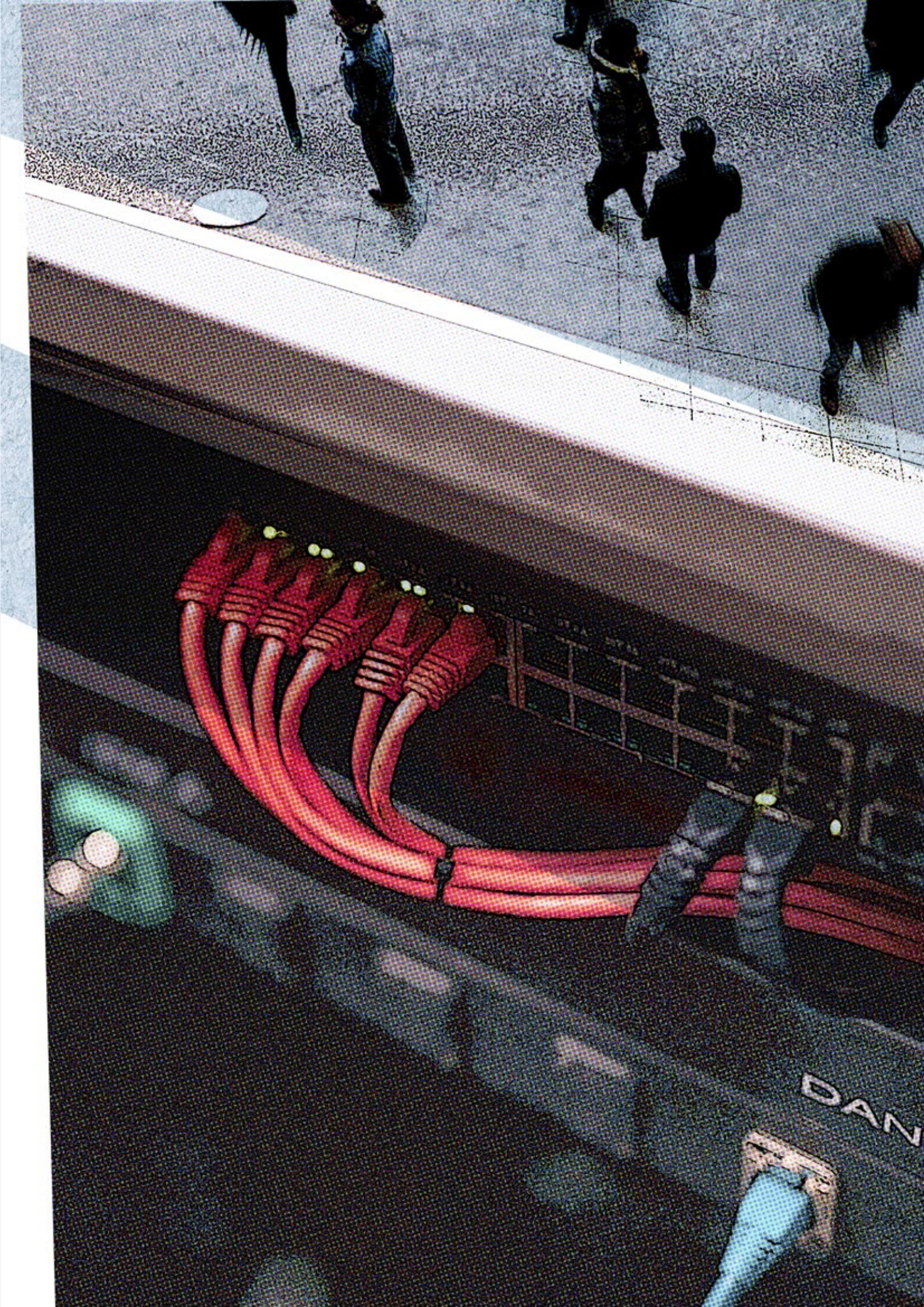
CFCS' opgave som national it-sikkerhedsmyndighed indebærer, at centret oplyser, vejleder og rådgiver danske myndigheder og virksomheder om it-sikkerhed og fungerer som nationalt kompetencecenter på cybersikkerhedsområdet. Som national it-sikkerhedsmyndighed er det tillige CFCS' opgave at sikkerhedsgodkende 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.


DAN

2. Tilsynet med Efterretningstjenesterne

Tilsynet er et særligt uafhængigt kontrolorgan, der fører tilsyn med, at PET, FE og CFCS 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 2019:

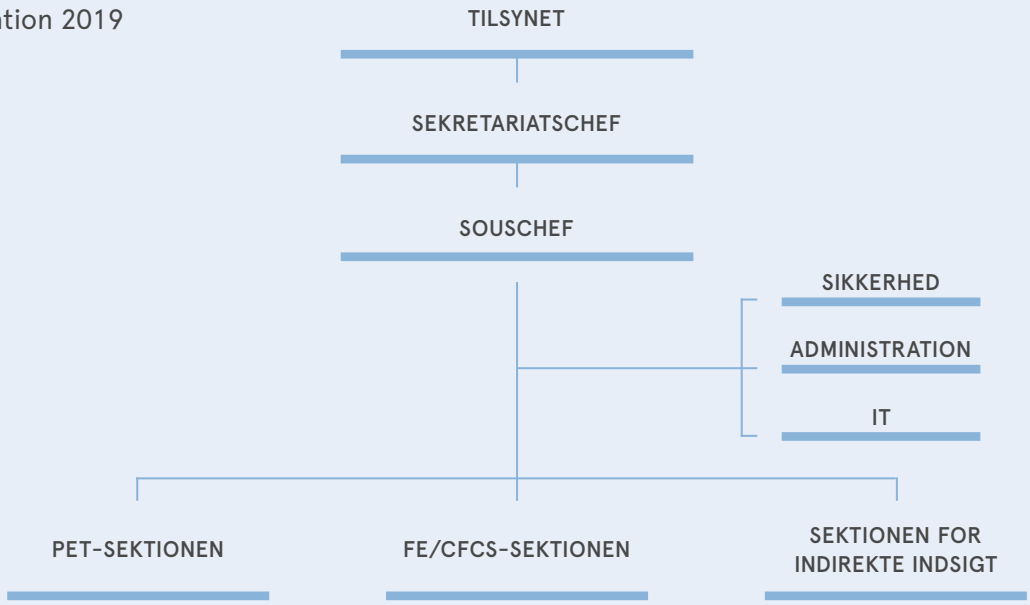
- Landsdommer Michael Kistrup, Østre Landsret (formand)
- Bestyrelsesformand Erik Jacobsen, Roskilde Universitet
- Juridisk chef Pernille Christensen, Kommunernes Landsforening
- Professor Henrik Udsen, Københavns Universitet
- Professor Rebecca Adler-Nissen, Københavns Universitet

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 2019 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, FE/CFCS og anmodninger om indirekte indsigt. Med henblik på at sikre faglig koordinering og erfaringsudveksling arbejder tilsynets medarbejdere på tværs af sektionerne.

Organisation 2019



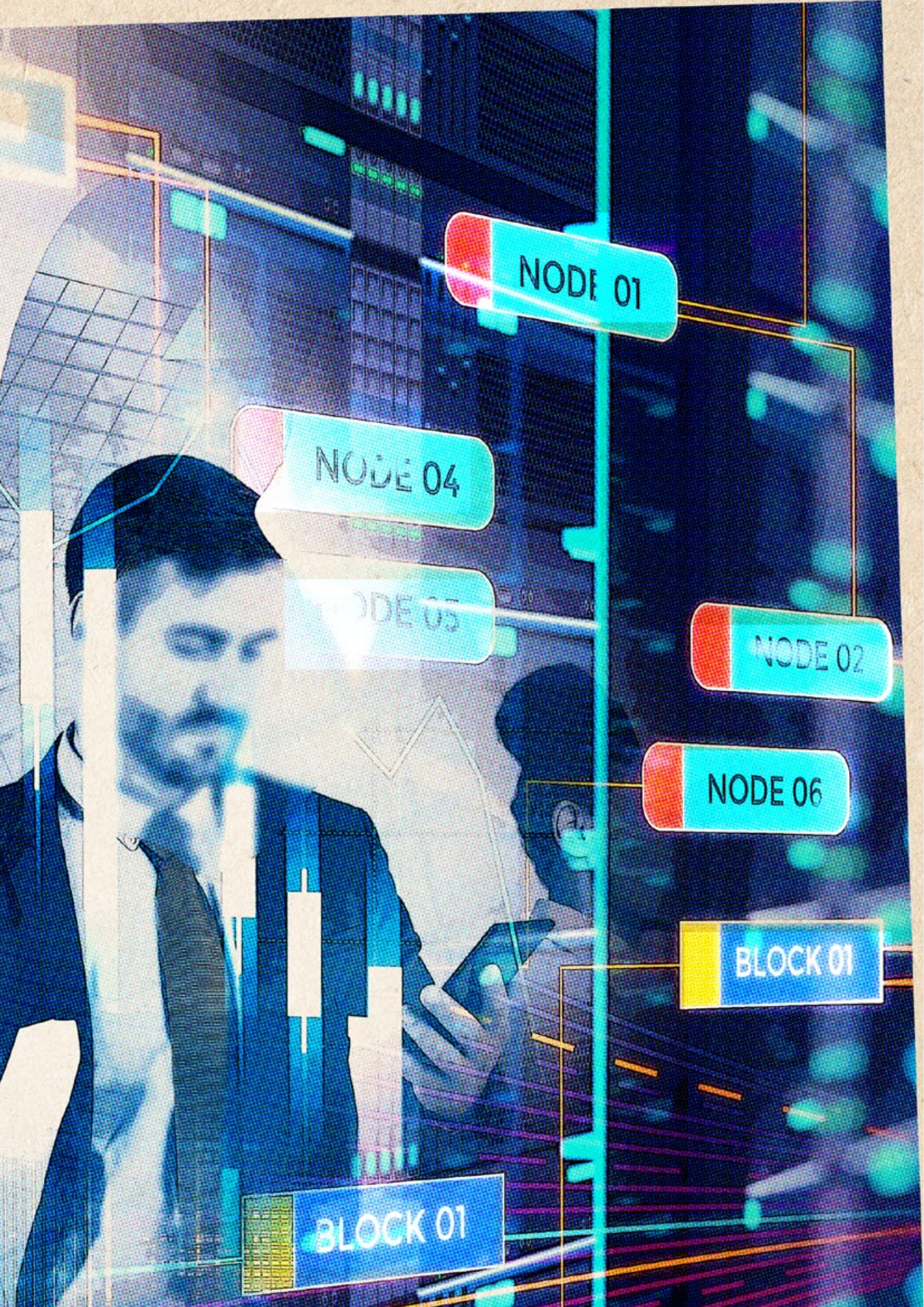
2.1 Tilsynets opgaver i forhold til CFCS

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.


NODE 01
NODE 04
NODE 02
NODE 06
BLOCK 01
BLOCK 01

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.

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 juni 2019. Redegørelsen blev offentliggjort i juli 2019.

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)

3.1 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).

Bestemmelsens 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.

Af lovens § 17, stk. 2, fremgår, 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.

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 udenrigsefterretningstjeneste 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 2019
Center for Cybersikkerhed
Udgivet af Tilsynet med Efterretningstjenesterne, august 2020

Layout + illustrationer: Eckardt ApS
Portrætfotos: Lars Engelgaar

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

Medlemmer af Tilsynet med Efterretningstjenesterne

Landsdommer Michael Kistrup, Østre Landsret (formand)
Bestyrelsesformand Erik Jacobsen, Roskilde Universitet
Juridisk chef Pernille Christensen, Kommunernes Landsforening
Professor Henrik Udsen, Københavns Universitet
Professor Rebecca Adler-Nissen, Københavns Universitet

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