tet

Tilsynet med Efterretningstjenesterne

Årsredegørelse 2023

Center for Cybersikkerhed

TIL FORSVARSMINISTEREN

I overensstemmelse med § 24 i lov om Center for Cybersikkerhed (lovbekendtgørelse nr. 836 af 7. august 2019) afgiver Tilsynet med Efterretningstjenesterne (TET) hermed redegørelse om sin virksomhed vedrørende Center for Cybersikkerhed (CFCS) for 2023. Redegørelsen skal offentliggøres.

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

TET 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 TET 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.

København, maj 2024

Pernille Christensen

Henrik Udsen

Jesper Fisker

Rebecca Adler-Nissen

Michael Kistrup

INDHOLD

1. Indledende bemærkninger ... 3

2. Generelt om TETs kontrolvirksomhed ... 4
2.1 Generelle forudsætninger for TETs kontrol og tilsynets forventninger til PET, FE, CFCS og PPNR ... 5
2.2 Skala for TETs bemærkninger ... 8
2.3 Kontrolmetode ... 9

3. TETs kontrol i 2023 ... 14
3.1 Sammenfatning af TETs kontrol i 2023 ... 15
3.2 Gennemførte kontroller af CFCS i 2023 ... 16
3.2.1 Kontrol af CFCS' behandling af oplysninger i kommunikationssystemer ... 16
3.2.2 Kontrol af CFCS' behandling af oplysninger i separate it-miljøer og analyseværktøjer ... 16
3.2.3 Kontrol af CFCS' behandling af oplysninger på drev ... 17
3.2.4 Kontrol af CFCS' behandling af oplysninger i andre systemer ... 17
3.2.5 Kontrol af CFCS' udveksling af oplysninger med den øvrige del af FE ... 17
3.2.6 Kontrol af CFCS' interne kontrol ... 18
3.2.7 Opfølgning på TETs kontrol af CFCS i 2022 ... 18
3.2.8 TETs tekniske undersøgelser og kortlægning af CFCS' it-landskab ... 19
3.3 CFCS' sagsbehandlingstider i 2023 ... 19
3.4 Sager forelagt forsvarsministeren til afgørelse ... 19

4. Eksempler på CFCS' håndtering af cyberangreb ... 22

5. Statistik vedrørende CFCS' behandling af oplysninger ... 24

APPENDIKS

1. Om Center for Cybersikkerhed ... 27

2. Om Tilsynet med Efterretningstjenesterne ... 28
2.1 TETs opgaver i forhold til CFCS ... 29
2.2 TETs adgang til oplysninger i CFCS ... 30
2.3 TETs reaktionsmuligheder ... 30

3. Retsgrundlag ... 32
3.1 CFCS' netsikkerhedstjeneste ... 32
3.1.1 Om CFCS' netsikkerhedstjeneste, jf. CFCS-lovens § 3 ... 32
3.2 Indgreb i meddelelseshemmeligheden og edition ... 33
3.2.1 Om indgreb i meddelelseshemmeligheden, jf. CFCS-lovens §§ 4-6 c ... 33
3.2.2 Om edition, jf. CFCS-lovens § 7 ... 34
3.3 Behandling af personoplysninger ... 34
3.3.1 Om behandling af personoplysninger, jf. CFCS-lovens §§ 9-14 ... 34
3.3.2 Om sikkerhedsforanstaltninger i forbindelse med behandling af personoplysninger, jf. CFCS-lovens § 18 ... 36
3.4 Analyse og sletning af data omfattet af CFCS-lovens kapitel 4 ... 36
3.4.1 Om analyse af data, jf. CFCS-lovens § 15 ... 36
3.4.2 Om sletning af data, jf. CFCS-lovens § 17 ... 37
3.5 Videregivelse og udveksling af oplysninger omfattet af CFCS-lovens kapitel 4 ... 38
3.5.1 Om videregivelse, jf. CFCS-lovens § 16 ... 38
3.5.2 Om udveksling af data med FE, jf. CFCS-cirkulærets § 2 ... 40

1. INDLEDENDE BEMÆRKNINGER

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 sensornetværk. For at udføre denne samfundsvigtige funktion har CFCS i henhold til lovgivningen 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.

TETs kontrolvirksomhed bidrager til legitimeringen af CFCS' aktiviteter ved at styrke offentlighedens tillid til, at centrets aktiviteter er lovmedholdelige. Det er en forudsætning for en effektiv og retvisende kontrol, at TET får uhindret, fuldstændig og rettidig adgang til CFCS' materiale af betydning for tilsynets virksomhed.

Som det fremgår af nærværende redegørelse har TET i 2023 foretaget en omfattende og intensiv kontrol af CFCS. TETs kontrol har fokuseret på CFCS' behandling og videregivelse af data fra centrets sensornetværk, som danske myndigheder og virksomheder, der varetager samfundsvigtige funktioner, er tilkoblet.

I 2023 har TET tillige intensiveret sit internationale samarbejde. Offentliggørelsen af TETs standarder for sin kontrolvirksomhed har i det forgangne år resulteret i en øget international interesse for tilsynets metoder for planlægning og gennemførelse af kontrol af efterretningstjenester. TET har således fortsat sine multilaterale og bilaterale samarbejder med lignende myndigheder i udlandet. Særligt ønsker TET at fremhæve konsolideringen af det tætte samarbejde med canadiske *National Security and Intelligence Review Agency* (NSIRA), som i 2023 udmøntede sig i et besøg ved den canadiske søsterorganisation, hvor fokus var på gensidig kompetenceopbygning og effektivisering af kontrolmetode.

TET har i 2023 endvidere sammen med sine norske og svenske søsterorganisationer arrangeret og afholdt den årlige internationale konference *European Intelligence Oversight Conference 2023* (EIOC), ligesom tilsynet har bidraget med faglige indlæg til *International Intelligence Oversight Forum* (IIOF), der i 2023 blev afholdt i Washington DC.

Regeringen (Socialdemokratiet, Venstre og Moderaterne) og Socialistisk Folkeparti indgik i december 2023 Aftale om styrkelse af Tilsynet med Efterretningstjenesterne og undersøgelse af visse konkrete sager, som efter indgåelse af en bred politisk aftale om styrkelse af tilsynet med efterretningstjenesterne i februar 2024 er udmøntet i et lovforslag om ændring af blandt andet PET-loven. Lovforslaget forventes vedtaget i indeværende folketingssamling.

2

Generelt om TETs kontrol-virksomhed

2.1 Generelle forudsætninger for TETs kontrol og tilsynets forventninger til PET, FE, CFCS og PPNR

Tilsynet med Efterretningstjenesternes (TET) kontrolvirksomhed bidrager til legitimeringen af Politiets Efterretningstjenestes (PET), Forsvarets Efterretningstjenestes (FE), Center for Cybersikkerheds (CFCS) og Politiets PNR-enheds (PPNR) aktiviteter ved at styrke offentlighedens tillid til, at disse aktiviteter er lovmedholdelige.

TETs virke er bestemt ved lov, herunder

- at tilsynet efter klage eller af egen drift påser, at PET, FE, CFCS og PPNR behandler personoplysninger i overensstemmelse med lovgivningen,
- at tilsynet hos PET, FE, CFCS og PPNR kan kræve enhver oplysning og alt materiale, der er af betydning for tilsynets virksomhed,
- at tilsynet til enhver tid har adgang til alle lokaler, hvorfra der er adgang til de oplysninger som behandles, eller hvor tekniske hjælpemidler anvendes,
- at tilsynet kan afkræve PET, FE, CFCS og PPNR skriftlige udtalelser om faktiske og retlige forhold af betydning for tilsynets kontrolvirksomhed,
- at PET, FE, CFCS eller PPNR – såfremt disse undtagelsesvist beslutter ikke at følge en henstilling i en udtalelse fra tilsynet – uden unødigt ophold skal forelægge sagen for henholdsvis justitsministeren eller forsvarsministeren til afgørelse,
- at tilsynet underretter henholdsvis justitsministeren og forsvarsministeren om forhold, som ministrene efter tilsynets opfattelse bør have kendskab til, og
- at tilsynet årligt skal afgive redegørelser om sin virksomhed, som skal offentliggøres.

Hvis PET, FE, CFCS eller PPNR undlader til fulde at efterleve disse grundlæggende forudsætninger for en effektiv og retvisende kontrol, vil det i væsentlig grad svække TETs muligheder for at kontrollere tjenesternes, centrets og enhedens lovmedholdelighed og herved bidrage til myndighedernes legitimitet over for offentligheden.

TET har følgende forventninger til PET, FE, CFCS og PPNR i opfyldelsen af disse krav:

TETs adgang til oplysninger

TET forventer, at PET, FE, CFCS og PPNR giver tilsynet uhindret, fuldstændig og rettidig adgang til alt materiale, som er relevant for at tilsynet kan gennemføre en korrekt og effektiv kontrol.

TET forventer, at PET, FE, CFCS og PPNR sikrer, at tilsynet har de rette brugeradgange til tjenesternes, centrets og enhedens it-infrastruktur, som sikrer direkte og uhindret adgang til relevante oplysninger for tilsynets kontrol.

TET forventer i de tilfælde, hvor der af tekniske årsager ikke kan gives fulde brugerrettigheder til udvalgte dele af PETs, FEs, CFCS' eller PPNRs it-infrastruktur, at tilsynet oplyses om

- karakteren og omfanget af den del af it-infrastrukturen, som tilsynet ikke egenhændigt har adgang til, og
- karakteren og omfanget af data, som behandles i den del af it-infrastrukturen, som tilsynet ikke egenhændigt har adgang til.

Uhindret, fuldstændig og rettidig adgang til materiale af betydning for TETs virksomhed er afgørende for en effektiv og retvisende kontrol.

PET, FE, CFCS eller PPNR vil undtagelsesvist kunne afgive udtalelse omkring undladelse af kontrol af udvalgte oplysninger. For at TETs lovbestemte adgang til oplysninger iagttages, er det imidlertid alene tilsynet, der har beslutningskompetencen om, hvorvidt udvalgte oplysninger kan undlades i forbindelse med en kontrol.

Såfremt TET ikke har mulighed for at verificere, at de pågældende oplysninger, som PET, FE, CFCS eller PPNR ønsker undladt i forbindelse med en kontrol, ikke er relevante for tilsynets kontrol vil dette udgøre en væsentlig risiko for omgåelse af loven.

Besvarelse af TETs høringer

TET forventer, at PETs, FEs, CFCS' og PPNRs høringssvar er fuldstændige, gennemsigtige og uforbeholdne.

TET forventer, at PET, FE, CFCS og PPNR oplyser tilsynet om eksistensen af øvrigt relevante oplysninger eller materiale af betydning for kontrollen, som tjenesterne, centret eller enheden måtte erkende, at tilsynet ikke har indsigt i.

TET forventer, at PETs, FEs, CFCS' og PPNRs høringssvar afgives rettidigt og inden for de tidsrammer, som fremgår af tilsynets proces for høring af tjenesterne, centret og enheden (se proces for høring af PET, FE, CFCS og PPNR i Standarder for TETs virksomhed).

Med henblik på at sikre en effektiv og retvisende kontrol fremsender TET målrettede anmodninger om udtalelser om faktiske og retlige forhold af betydning for tilsynets kontrolvirksomhed.

TET har beslutningskompetencen i afgørelsen af, om udvalgte oplysninger er relevante for kontrollen, hvorfor PETs, FEs, CFCS' og PPNRs høringssvar skal være fuldstændige, gennemsigtige og uforbeholdne.

PET, FE, CFCS eller PPNR må således ved besvarelse af TETs høringer ikke selvstændigt foretage en vurdering af, om udvalgte anmodninger om oplysninger er relevante for tilsynets kontrol.

Opfølgning på TETs kontrol

TET forventer – såfremt PET, FE, CFCS eller PPNR måtte have bemærkninger til resultatet af tilsynets enkeltvise kontroller – at disse fremsendes til tilsynet inden for den frist, som er angivet i tilsynets opfølgningsbrev.

TET forventer – såfremt PET, FE, CFCS eller PPNR undtagelsesvist måtte beslutte ikke at følge en henstilling fra tilsynet – at tjenesten, centret eller enheden opfylder deres oplysningspligt og uden unødigt ophold forelægger sagen for henholdsvis justitsministeren eller forsvarsministeren til afgørelse.

Praksis, som TET har vurderet ikke er lovmedholdelig, og hvor PET, FE, CFCS eller PPNR er enige heri, skal håndteres straks, og uenighed om fortolkningen af lovgrundlaget bør afklares uden unødigt ophold. Det er derfor afgørende, at PET, FE, CFCS eller PPNR rettidigt responderer på TETs henstillinger, herunder om nødvendigt ved at forelægge en given sag for henholdsvis justitsministeren og forsvarsministeren til afgørelse.

2.2 Skala for TETs bemærkninger

TETs bemærkninger tager udgangspunkt i følgende skala:

BEMÆRKNINGER	BAGGRUND FOR BEMÆRKNINGER
[...] ***giver ikke anledning til bemærkninger***	Anvendes når TET er enig med myndigheden i, hvordan loven generelt eller konkret administreres.
TET finder ***ikke*** *på det foreliggende grundlag, at* ***det er muligt at vurdere*** [...]	Anvendes når TETs prøvelsesmuligheder er begrænset enten af faktiske eller juridiske forhold.
TET finder det ***bemærkelsesværdigt*** [...]	Anvendes om forhold i myndigheden eller lovgivningen, som ikke stemmer overens med det almindelige eller umiddelbare indtryk, som en udenforstående har.
TET 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 TET har været forhindret i at udøve sin virksomhed i en periode af en vis varighed.
TET kan ***konstatere*** [...]	Anvendes om forhold hvor der er konstateret egentlige lovbrud af enkeltstående karakter eller brud på interne retningslinjer.
TET finder det ***kritisabelt*** [...]	Anvendes om forhold hvor der er konstateret ikke uvæsentlige lovbrud eller hvor TET har været forhindret i at udøve sin virksomhed i en længere periode.
TET finder det ***overordentligt kritisabelt*** [...]	Anvendes om forhold hvor der er konstateret alvorlige lovbrud eller hvor TET har været forhindret i at udøve sin virksomhed i en længere periode, uden at myndigheden har udvist vilje til at sikre den fornødne afhjælpning heraf.

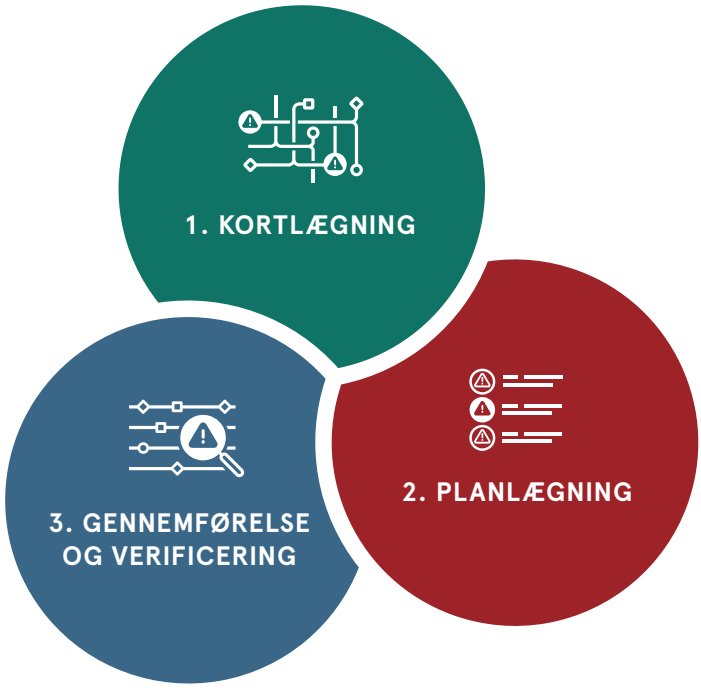
2.3 Kontrolmetode

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

TETs kontrol af PET, FE, CFCS og PPNR forudsætter kendskab til myndighedernes it-infrastruktur, prioritering af tilsynets ressourcer og effektive metoder til gennemførelse af kontrollen.

TET kan alene kontrollere de dele af PET, FE, CFCS og PPNR, som tilsynet har kendskab til. Endvidere har TET ikke ressourcer til at foretage en fuldstændig kontrol af alle dele af PET, FE, CFCS og PPNR. Endelig skal TETs kontroller kunne dokumentere forholdene i PET, FE, CFCS og PPNR med et begrænset ressourceforbrug.

TETs standarder har til formål at håndtere disse grundlæggende udfordringer. Derfor består TETs arbejde overordnet af tre delelementer:



TETs 1 kortlægning af it-infrastruktur i henholdsvis PET, FE, CFCS og PPNR har til formål at give tilsynet det nødvendige kendskab til tjenesternes, centrets og enhedens tilvejebringelse, behandling og videregivelse af oplysninger.

TET sammenstiller og vurderer informationer om relevante dele af it-infrastrukturen med henblik på at skabe det rette grundlag for at kunne foretage fuldstændige risiko- og væsentlighedsvurderinger af samtlige processer og systemer i PET, FE, CFCS og PPNR.

TETs metode til kortlægning af it-infrastruktur er egenudviklet. Metoden er en videreudvikling af TETs indledende kortlægning af it-systemer i PET og FE i 2014-2015, som har afstedkommet et behov for både tilpasning, strukturering og formalisering af metode.

Valget af metode afspejler en afvejning mellem behov for teknisk detaljegrad i kortlægningen til at kunne understøtte TETs kontrolvirksomhed, mængden af it-ressourcer og niveauet af modenhed for it-governance i såvel tilsynet som PET, FE, CFCS og PPNR.

TETs 2 planlægning af kontroller for det kommende år har til formål at prioritere tilsynets ressourcer, således at kontrollen rettes mod de dele af PET, FE, CFCS og PPNR, hvor der vurderes at være den største risiko for lovbrud.

Planlægningen sker på baggrund af en årlig risiko- og væsentlighedsvurdering af processer og systemer (herefter kontrolobjekter) i PET, FE, CFCS og PPNR med det formål at vurdere risici for lovbrud ved tjenesternes, centrets og enhedens aktiviteter. TET udarbejder på den baggrund risikoanalyser, som danner grundlag for udvælgelsen af det kommende års kontroller. De udvalgte kontroller samles i kontrolplaner for PET, FE, CFCS og PPNR for det kommende år.

Formålet med risikoanalyserne er at sikre, at TETs kontrol fokuseres på områder, hvor der er størst risiko for lovbrud, samt at der tages højde for andre relevante faktorer, eksempelvis områder hvor tilsynets kontrol fra lovgivers side er tillagt særlig vægt, såsom reglerne om lovlig politisk virksomhed.

Områder hvor der vurderes at være en lavere risiko for lovbrud kontrolleres som hovedregel hvert femte år med henblik på at skabe fuldstændighed i kontrollen af PET, FE, CFCS og PPNR og sikre, at vurderingen af risiko for lovbrud på området fortsat er retvisende.

TETs kontroller 3 gennemføres løbende hen over året på baggrund af kontrolplanerne for henholdsvis PET, FE, CFCS og PPNR. TET fastlægger ikke metoder for de enkelte kontroller i forbindelse med udarbejdelsen af risikovurderinger og -analyser men først efter en forudgående teknisk og juridisk afdækning af det enkelte kontrolobjekt.

TET benytter sig af en række forskellige metoder i kontrollen af de enkelte kontrolobjekter, heriblandt fuldstændig kontrol, tilfældige eller målrettede stikprøver, indholdsscreening, inspektioner samt interview- og høringsbaserede kontroller.

TETs valg af kontrolmetode sker på baggrund af en konkret risikovurdering af kontrolobjektet, erfaringer fra tidligere kontroller samt de faktiske forhold, som tilsynet konstaterer i forbindelse med den specifikke kontrol. I den sammenhæng afholder TET forud for kontrol af ikke tidligere kontrollerede områder et opstartsmøde med relevante medarbejdere i PET, FE, CFCS eller PPNR med henblik på at sikre en tilstrækkelig politi- og/eller efterretningsfaglig samt teknisk og juridisk forståelse af området, således at kontrollen kan tilpasses og gennemføres hensigtsmæssigt.

Som en del af TETs gennemførelse af kontroller foretages tillige verificeringskontroller af PETs, FEs, CFCS' og PPNRs it-infrastruktur. Formålet er herved at sikre, at TETs kontrol beror på oplysninger fra PET, FE, CFCS og PPNR, hvis rigtighed tilsynet har efterprøvet.

Processerne for TETs 1 kortlægning, 2 planlægning samt 3 gennemførelse og verificering fremgår af følgende figur. Processerne er understøttet af løbende kvalitetssikring ved godkendelse på henholdsvis chefniveau og tilsynsniveau samt ved høringer af eksterne parter om juridiske, faktuelle eller klassifikationsmæssige forhold.


Se Standarder for TETs virksomhed (afsnit 1 - Kortlægning af it-infrastruktur)
Kortlægning af PETs, FEs, CFCS' og PPNRs it-infrastruktur
KVALITETSSIKRING
Ekstern høring om faktuelle forhold
KVALITETSSIKRING
Godkendelse på chefniveau
Se Standarder for TETs virksomhed (afsnit 2 - Risiko- og væsentlighedsvurdering)
Risiko- og væsentlighedsvurdering af PET, FE, CFCS og PPNR
KVALITETSSIKRING
Godkendelse på chefniveau
Forelæggelse af risiko- og væsentlighedsvurdering af PET, FE, CFCS og PPNR og beslutning om kontrolplaner for det kommende år
KVALITETSSIKRING
Drøftelse og godkendelse på tilsynsniveau
Se Standarder for TETs virksomhed (afsnit 3 - Metode, gennemførelse af kontrol og verificering af oplysninger)
Afklaring af kontroltype for samtlige planlagte kontroller
KVALITETSSIKRING
Godkendelse på chefniveau
Orientering af PET, FE, CFCS og PPNR om TETs kontrolplaner
Teknisk og juridisk afdækning af kontrolobjekter
KVALITETSSIKRING
Ekstern høring om juridiske og faktuelle forhold
Beslutning om metode for de enkelte kontroller
KVALITETSSIKRING
Godkendelse på chefniveau
Gennemførelse af kontroller
KVALITETSSIKRING
Godkendelse på chefniveau
Høring af PET, FE, CFCS eller PPNR i forbindelse med kontroller
KVALITETSSIKRING
Ekstern høring om juridiske og faktuelle forhold
Forelæggelse og afslutning af kontroller
KVALITETSSIKRING
Drøftelse og godkendelse på tilsynsniveau
Fremsendelse af opfølgningsbreve til PET, FE, CFCS eller PPNR
KVALITETSSIKRING
Ekstern kvalitetssikring ved eventuelle bemærkninger vedrørende kontrollen
Udarbejdelse af årlige redegørelser om PET og PPNR, FE samt CFCS
KVALITETSSIKRING
Drøftelse og godkendelse på tilsynsniveau
KVALITETSSIKRING
Ekstern kvalitetssikring ved høring om faktuelle eller klassifikationsmæssige forhold
Offentliggørelse af TETs årlige redegørelser

TETs direkte adgang til PETs, FEs, CFCS' og PPNRs systemer sikrer, at myndighederne ikke kan forudse, hvilke sager og oplysninger der bliver genstand for kontrol. I nogle tilfælde er det imidlertid nødvendigt for TET at varsle PET, FE, CFCS eller PPNR om tidspunktet og metoden for en kontrol, eksempelvis hvis tilsynet skal have adgang til særlige fysiske lokaliteter eller skal interviewe specifikke medarbejdere.

TET deler forud for påbegyndelsen af årets kontroller sine risikoanalyser og kontrolplaner med henholdsvis PET, FE, CFCS og PPNR med henblik på at sikre åbenhed om tilsynets vurdering af forholdene i myndighederne. Åbenheden giver endvidere PET, FE, CFCS og PPNR mulighed for at tage højde for TETs kontrol i tilrettelæggelsen af myndighedernes interne kontrol, hvilket bidrager til, at tilsynets kontrol og myndighedernes interne kontrol samlet dækker en større del af disses virksomhed. Endelig sikrer åbenheden, at PET, FE, CFCS og PPNR kan afsætte tilstrækkelige ressourcer til at betjene TET.

TET udarbejder desuden særskilte risikovurderinger og -analyser specifikt for tilsynets opgaver i relation til PET og FE efter den indirekte indsigtsordning, blandt andet med henblik på at sikre at tilsynets undersøgelser i forbindelse med anmodninger om indirekte indsigt er effektive og relevante.

For yderligere information om TETs kontrolmetodik henvises til tilsynets offentliggjorte standarder herfor, som findes på tilsynets hjemmeside.

3 TETs kontrol i 2023

3.1 Sammenfatning af TETs kontrol i 2023

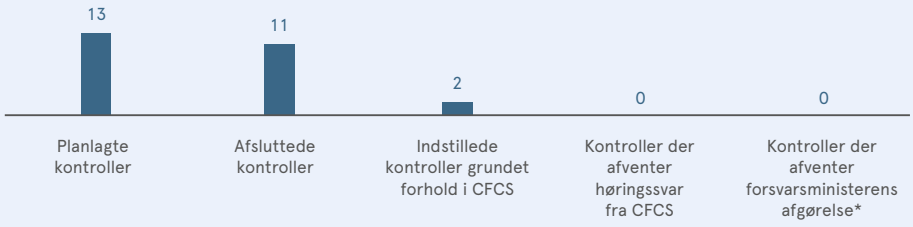
Tilsynet med Efterretningstjenesterne (TET) har i 2023 afsluttet 11 ud af 13 planlagte kontroller af Center for Cybersikkerhed (CFCS).

Resultatet af TETs kontroller er beskrevet i deres helhed i afsnit 3.2. I det følgende fremhæves centrale og principielle dele af redegørelsen.

- Ingen af de 11 kontroller af CFCS gav anledning til bemærkninger.
- TET besluttede at indstille to planlagte kontroller af CFCS' drevstrukturer i 2023, idet der fortsat ikke var etableret en løsning, som muliggør søgning i indholdet af drevstrukturerne.

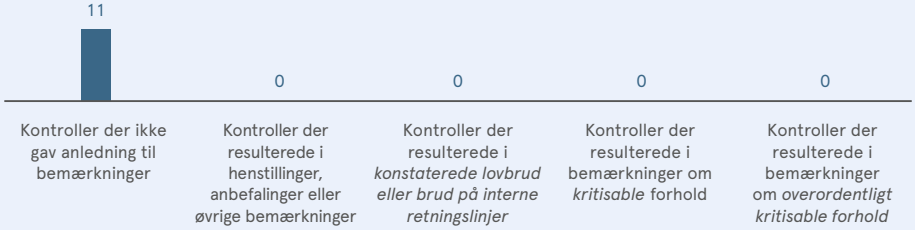
TET vurderede, at CFCS i 2023 havde foretaget de skridt for at fremme etableringen af løsningen, som havde været mulige for centret, og at forsinkelsen skyldtes udfordringer med eksterne leverancer (afsnit 3.2.3).

TETs kontrol af CFCS i 2023



* Se imidlertid afsnit 3.4

Resultater af TETs kontrol af CFCS i 2023



3.2 Gennemførte kontroller af CFCS i 2023

Med henblik på at kontrollere, at CFCS i forbindelse med behandling af oplysninger om fysiske personer overholder reglerne i CFCS-loven, har TET i 2023 foretaget kontrol af centrets

- behandling af oplysninger i kommunikationssystemer (afsnit 3.2.1),
- behandling af oplysninger i separate it-miljøer og analyseværktøjer (afsnit 3.2.2),
- behandling af oplysninger på drev (afsnit 3.2.3),
- behandling af oplysninger i andre systemer (afsnit 3.2.4),
- udveksling af oplysninger med den øvrige del af FE (afsnit 3.2.5) og
- interne kontrol (afsnit 3.2.6).

Endvidere gennemførte TET i 2023

- opfølgning på TETs kontrol af CFCS i 2022 (afsnit 3.2.7) og
- tekniske undersøgelser og kortlægning af centrets it-landskab (afsnit 3.2.8).

3.2.1 Kontrol af CFCS' behandling af oplysninger i kommunikationssystemer

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.

CFCS anvender kommunikationssystemer til videregivelse af oplysninger til relevante eksterne samarbejdspartnere, samt myndigheder og virksomheder tilsluttet centrets sensornetværk.

CFCS anvender ligeledes forskellige kommunikations- eller mailsystemer, som muliggør at medarbejdere i forskellige dele af centret kan udveksle oplysninger.

TET foretog i 2023 kontrol af CFCS' behandling af oplysninger i tre kommunikationssystemer. TETs kontrol fokuserede på oplysninger, som var omfattet af CFCS-lovens kapitel 4, og som på tidspunktet for tilsynets kontrol burde have været slettet, jf. CFCS-lovens § 17, stk. 2.

TETs bemærkninger

TETs kontrol af CFCS' behandling af oplysninger i kommunikationssystemer i 2023 gav ikke anledning til bemærkninger.

3.2.2 Kontrol af CFCS' behandling af oplysninger i separate it-miljøer og analyseværktøjer

CFCS anvender en række separate it-miljøer og analyseværktøjer i forbindelse med centrets tekniske analyse af eksempelvis cyberangreb, malware, og phishing. CFCS behandler og

opbevarer oplysninger i disse it-miljøer og analyseværktøjer i forbindelse med centrets analyse heraf. Oplysningerne vil i nogle tilfælde stamme fra CFCS' sensornetværk, men kan også være tilvejebragt fra åbne kilder, eksempelvis på internettet.

TET foretog i 2023 kontrol af CFCS' behandling af oplysninger i tre analyseværktøjer.

TETs bemærkninger

TETs kontrol af CFCS' behandling af oplysninger i separate it-miljøer og analyseværktøjer i 2023 gav ikke anledning til bemærkninger.

3.2.3 Kontrol af CFCS' behandling af oplysninger på drev

CFCS anvender drev til opbevaring af oplysninger i forbindelse med mange forskellige dele af centrets virksomhed.

TET planlagde i 2023 at foretage to kontroller af forskellige drevstrukturer i CFCS.

TETs bemærkninger

TET besluttede at indstille to planlagte kontroller af CFCS' drevstrukturer i 2023, idet der fortsat ikke var etableret en løsning, som muliggør søgning i indholdet af drevstrukturerne.

TET vurderede, at CFCS i 2023 havde foretaget de skridt for at fremme etableringen af løsningen, som var mulige for centret, og at forsinkelsen skyldtes udfordringer med eksterne leverancer.

TETs øvrige kontrol af CFCS' behandling af oplysninger på drev i 2023 gav ikke anledning til bemærkninger.

3.2.4 Kontrol af CFCS' behandling af oplysninger i andre systemer

CFCS anvender i forbindelse med centrets virksomhed en lang række forskellige systemer til at opbevare og behandle oplysninger. Dette kan eksempelvis være journalsystemer, arbejdsstationer mv.

TET foretog i 2023 kontrol af CFCS' behandling af oplysninger i andre systemer ved kontrol af arbejdsstationer i centret.

TETs bemærkninger

TETs kontrol af CFCS' behandling af oplysninger i andre systemer i 2023 gav ikke anledning til bemærkninger.

3.2.5 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, der er omfattet af kapitel 4 i lov om Center for Cybersikkerhed, mellem centret og den øvrige del af tjenesten 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, der er omfattet af kapitel 4 i lov om Center for Cybersikkerhed, fra CFCS til FE.

TET foretog i 2023 kontrol af CFCS' udveksling af oplysninger med den øvrige del af FE.

TETs bemærkninger

TETs kontrol af CFCS' udveksling af oplysninger, der er omfattet af kapitel 4 i lov om Center for Cybersikkerhed, med den øvrige del af FE i 2023 gav ikke anledning til bemærkninger.

3.2.6 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 risikoanalyse af centrets overholdelse af lovkrav samt en plan for den interne kontrol i det følgende år. CFCS orienterer løbende TET om tilrettelæggelsen af den interne kontrol samt resultatet heraf, herunder ved fremsendelse af centrets risikoanalyse og kontrolplan.

TET foretog i 2023 kontrol af CFCS' interne kontrol. Kontrollen omfattede CFCS' interne kontrol i 2022 samt centrets planlægning heraf for 2023.

CFCS orienterede i september 2023 TET om centrets

- risikoanalyse vedrørende overholdelse af lovkrav og
- kontrolplan for 2023.

CFCS orienterede i 2023 derudover løbende TET om centrets interne kontrol.

TETs bemærkninger

TETs kontrol af CFCS' interne kontrol i 2023 gav ikke anledning til bemærkninger.

3.2.7 Opfølgning på TETs kontrol af CFCS i 2022

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

TET foretog i 2023 opfølgning på tilsynets kontrol af CFCS i 2022.

TET foretog en gennemgang af de oplysninger, som CFCS i forbindelse med tilsynets kontroller i 2022 erklærede sig enig i at slette samt centrets opfølgning på de anmodninger og anbefalinger, som tilsynet afgav over for centret på baggrund af tilsynets kontroller i 2022. Gennemgangen skete endvidere med henblik på at konstatere, om CFCS havde foretaget de ændringer, som centret i forbindelse med kontrollerne i 2022 havde tilkendegivet over for TET, at centret ville foretage.

TETs bemærkninger

TETs opfølgning på tilsynets kontrol af CFCS i 2022 gav ikke anledning til bemærkninger.

3.2.8 TETs tekniske undersøgelser og kortlægning af CFCS' it-landskab

CFCS' it-systemer og underliggende databaser, hvori der behandles oplysninger, udgør et komplekst og dynamisk landskab af forskellige teknologier og datatyper. For at kunne navigere i dette komplekse it-landskab og løse TETs primære opgaver, har tilsynet i 2023 gennemgået og verificeret omfattende dele af CFCS' it-landskab, og arbejder løbende med at sikre et opdateret kendskab til centrets systemer.

Det er en forudsætning for meningsfuld kontrol af CFCS, at TET har kendskab til centrets samlede it-infrastruktur, således at kontrollen kan målrettes de dele af infrastrukturen, som udgør størst risiko for behandling i strid med CFCS-lovgivningen.

TET foretog i 2023 verificeringskontroller og inspektioner af CFCS' it-infrastruktur ved kortlægning af centrets serverinfrastruktur.

TETs bemærkninger

TETs kortlægning af CFCS' serverinfrastruktur i 2023 gav ikke anledning til bemærkninger.

3.3 CFCS' sagsbehandlingstider i 2023

TET fremsendte syv høringer til CFCS i forbindelse med tilsynets kontrolvirksomhed i 2023. CFCS besvarede fem af TETs høringer inden for den angivne frist og to efter udløbet af den angivne frist. CFCS' gennemsnitlige sagsbehandlingstid for besvarelse af høringer, som først blev besvaret efter udløbet af fristen, var på fem arbejdsdage.

3.4 Sager forelagt forsvarsministeren til afgørelse

TET kan som led i sin kontrol af CFCS afgive udtalelser over for centret, hvori tilsynet blandt andet kan tilkendegive sin opfattelse af, om centret overholder CFCS-lovens regler.

TET afgiver ved afslutningen af hver kontrol en udtalelse til CFCS, hvor resultatet af tilsynets kontrol beskrives. Udtalelsen kan herudover indeholde en beskrivelse af et eller flere tiltag, som TET vurderer at CFCS bør foretage. Hvis CFCS undtagelsesvist måtte beslutte ikke at følge en henstilling i en udtalelse fra TET, skal centret underrette tilsynet herom og uden unødigt ophold forelægge sagen for forsvarsministeren til afgørelse. TETs reaktionsmuligheder over for CFCS er beskrevet nærmere i afsnit 2.3 i appendiks samt i CFCS-lovens § 21.

Følgende skema giver et overblik over sager forelagt forsvarsministeren siden TETs oprettelse i 2014:

SPØRGSMÅL	DATO FOR FORELÆGGELSE	STATUS
Hvorvidt CFCS i forbindelse med overholdelsen af CFCS-lovens § 18 for hvert af centrets systemer er forpligtet til at foretage vurdering af, hvilke foranstaltninger der kan tilvejebringe et tilstrækkeligt sikkerhedsniveau. Nærmere behandlet i TETs årsredegørelse for 2022 (afsnit 2.2.7).	4. august 2023	Afventer forsvarsministerens afgørelse.
Hvorvidt forsvarsministerens afgørelse af 11. august 2021 vedrørende sletning af data fra centrets sensornetværk kun er gældende, når sensordata opbevares i alarmenhederne og CFCS' centrale analyseplatform, eller er gældende i alle tilfælde, hvor CFCS opbevarer sensordata i relevante behandlingssystemer, eksempelvis lokalt på en medarbejders arbejdsstation. Nærmere behandlet i TETs årsredegørelse for 2022 (afsnit 2.2.3).	1. august 2023	Afventer forsvarsministerens afgørelse.
Hvorvidt data fra CFCS' sensornetværk i henhold til CFCS-lovens § 17, stk. 1, skal slettes umiddelbart efter, at undersøgelsen af den konkrete hændelse, der har forårsaget indhentningen, er afsluttet. Nærmere behandlet i TETs redegørelse for 2021 (afsnit 2).	11. august 2020	Afgjort den 11. august 2021. Forsvarsministeren fandt, 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, eksempelvis stationære data, som er tilvejebragt i henhold til CFCS-lovens § 5. Stationære data omfatter data, som opbevares på blandt andet servere, lagerenheder, mobile enheder eller lignende, og som i modsætning til sensordata ikke udgør kommunikation mellem netværk.

4

Eksempler på CFCS' håndtering af cyberangreb

Ifølge forarbejderne til CFCS-loven skal TETs 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 2023:

CFCS har til opgave at beskytte de vigtige dele af det danske samfund mod cyberangreb. I praksis løses denne opgave ved, at CFCS opdager, analyserer og bidrager til at imødegå sikkerhedshændelser hos myndigheder og virksomheder med samfundsvigtig karakter, der er tilsluttet CFCS' sensornetværk, eller som anmoder om CFCS' bistand. Ved siden af data fra sensornetværket samt kommercielt anskaffet og åbent tilgængelige data, gør CFCS i sin opgaveløsning også brug af informationer frembragt gennem FE's internationale efterretningsarbejde.

I 2023 har CFCS håndteret en lang række sikkerhedshændelser for myndigheder og virksomheder i og uden for sensornetværket. Hændelserne omfattede systematisk udnyttelse af kendte eller hidtil ukendte sårbarheder, datalæk, rekognoscering, spear phishing og forsøg på brute forcing. En del af hændelserne omfattede også kompromitteringer i form af spionage og datatyveri samt ransomwareangreb med kryptering af data til følge. CFCS har i 2023 observeret angreb og forsøg på angreb fra både statsstøttede og kriminelle cyberaktører.

Angrebsforsøg via phishing er fortsat en alvorlig trussel mod tilsluttede myndigheder og virksomheder. Det kan eksempelvis være mails fra en ondsindet aktør, der forsøger at lokke en modtager til at aktivere eller tilgå indhold i mailen, som enten kan føre til inficeringer eller franarre login-oplysninger fra ofret. Desuden observerer CFCS løbende forskellige typer forsøg på at udnytte fejlkonfigurationer og offentligt kendte sårbarheder i softwaretjenester, som er eksponeret mod internettet.

5 Statistik vedrørende CFCS' behandling af oplysninger

Det fremgår af forarbejderne til CFCS-loven, at TETs 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 2023:

TABEL 1 – VIDEREGIVELSER OG UDVEKSLINGER	2023
Videregivelser	29
Udvekslinger	16
Total	**45**

TABEL 2 – BEKRÆFTEDE SIKKERHEDSHÆNDELSER* EFTER ALVORLIGHEDSGRAD	2023
Alvorlige	2
Større	8
Moderate	12
Mindre	193
Ingen**	993
Falske positive***	1.256
Total	**2.464**

* Sikkerhedshændelser defineres i overensstemmelse med § 2, nr. 1, i lov om Center for Cybersikkerhed.
** Kategorien "Ingen" inkluderer alle de sikkerhedshændelser, som ikke har haft en indvirkning på kunden.
*** Falske positive dækker over mistanke om en sikkerhedshændelse der ved nærmere analyse viser sig ikke at være en sikkerhedshændelse

TABEL 3 – AKTINDSIGTSSAGER	2023
Fuld aktindsigt	10
Delvis aktindsigt	5
Afslag på aktindsigt	3
Ingen omfattede dokumenter lokaliseret	4
Total	**22**

TABEL 4 – BEHANDLING AF PERSONOPLYSNINGER	2023
Klager til CFCS over behandling af personoplysninger	0*
Klagesager modtaget i TET	0

* CFCS har ikke kendskab til, at der er modtaget klager over centrets behandling af personoplysninger.

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 (TET), 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.

2. OM TILSYNET MED EFTERRETNINGSTJENESTERNE

TETS VIRKSOMHED

Personale i 2023 (ansatte)	8
Finanslovsbevilling i 2023 (mio. kr.)	10,1

Tilsynet med Efterretningstjenesterne (TET) er et uafhængigt kontrolorgan, der fører tilsyn med, at Politiets Efterretningstjeneste (PET), Forsvarets Efterretningstjeneste (FE), Center for Cybersikkerhed (CFCS) og Politiets PNR-enhed (PPNR) behandler personoplysninger i overensstemmelse med lovgivningen.

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

TET 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.

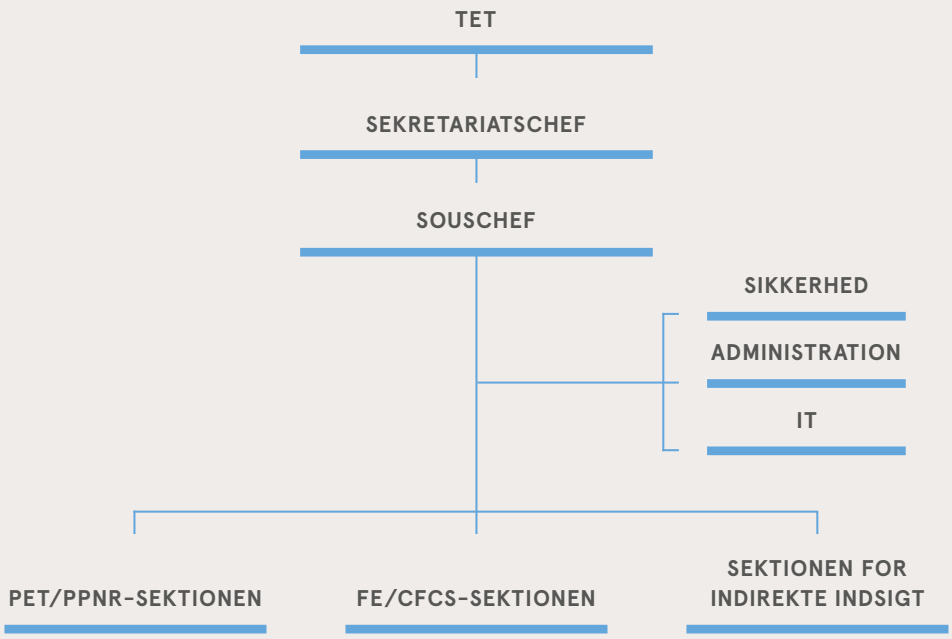
Medlemmerne var ved udgangen af 2023:

- Landsdommer Michael Kistrup, Østre Landsret (formand)
- Juridisk chef Pernille Christensen, Kommunernes Landsforening
- Professor Henrik Udsen, Københavns Universitet
- Professor Rebecca Adler-Nissen, Københavns Universitet
- Direktør Jesper Fisker, Kræftens Bekæmpelse

Medlemmerne udpeges for en periode på fire år med mulighed for genbeskikkelse for yderligere fire år. Ved TETs 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.

TET bistås af et sekretariat, der alene er undergivet tilsynets instruktion. TET bestemmer selv, hvem der skal ansættes til sekretariatet, herunder hvilken uddannelsesmæssig baggrund og øvrige kvalifikationer de pågældende skal have. Ved udgangen af 2023 bestod sekretariatet af en sekretariatschef, der varetager den daglige ledelse, en souschef, tre jurister, to it-konsulenter og en kontorfunktionær.

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



2.1 TETs opgaver i forhold til CFCS

Ifølge CFCS-loven skal TET 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. TET 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.

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

TET 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 TET vil tage sager op af egen drift. Der er ikke givet nærmere retningslinjer for TETs udførelse af sin kontrol.

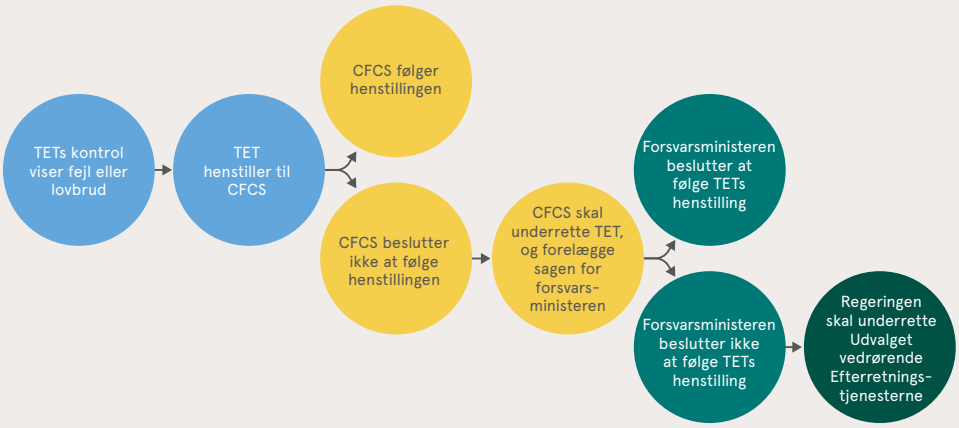
2.2 TETs adgang til oplysninger i CFCS

TET kan hos CFCS kræve enhver oplysning og alt materiale, der er af betydning for tilsynets virksomhed, og har til enhver tid adgang til alle lokaler, hvorfra der er adgang til de oplysninger, som behandles, eller hvor tekniske hjælpemidler anvendes. TET 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 TET, hvorfra tilsynet på egen hånd kan foretage søgninger i centrets it-systemer.

2.3 TETs reaktionsmuligheder

TET har ikke kompetence til at påbyde CFCS bestemte foranstaltninger i forhold til behandling af oplysninger. TET kan derimod afgive udtalelser over for CFCS, hvori tilsynet blandt andet kan tilkendegive sin opfattelse af, om centret overholder reglerne om behandling af oplysninger. TET afgiver ved afslutningen af hver kontrol en udtalelse til CFCS, hvor resultatet af tilsynets kontrol beskrives. Udtalelsen kan herudover indeholde en beskrivelse af et eller flere tiltag, som TET vurderer at CFCS bør foretage. Hvis CFCS undtagelsesvist måtte beslutte ikke at følge en henstilling i en udtalelse fra TET, skal centret underrette tilsynet herom og uden unødigt ophold forelægge sagen for forsvarsministeren til afgørelse.



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

TET afgiver en årlig redegørelse om sin virksomhed til forsvarsministeren. Redegørelsen, der 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 TET måtte have valgt særligt at interessere sig for. Redegørelsen skal indeholde statistiske oplysninger om CFCS' behandling af person-

oplysninger, 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. TET 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.

TET afgav senest en årlig redegørelse om sin virksomhed til forsvarsministeren i juni 2023. Redegørelsen blev offentliggjort i november 2023.

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 centrets 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 domæ-

nenavne 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 stammer 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 TETs 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 TET 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 2023
Center for Cybersikkerhed
Udgivet af Tilsynet med Efterretningstjenesterne, maj 2024
Layout + illustrationer: Eckardt ApS
Portrætfotos: Lars Engelgaar / Tomas Bertelsen

Publikationen kan downloades fra TETs 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
Direktør Jesper Fisker, Kræftens Bekæmpelse

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