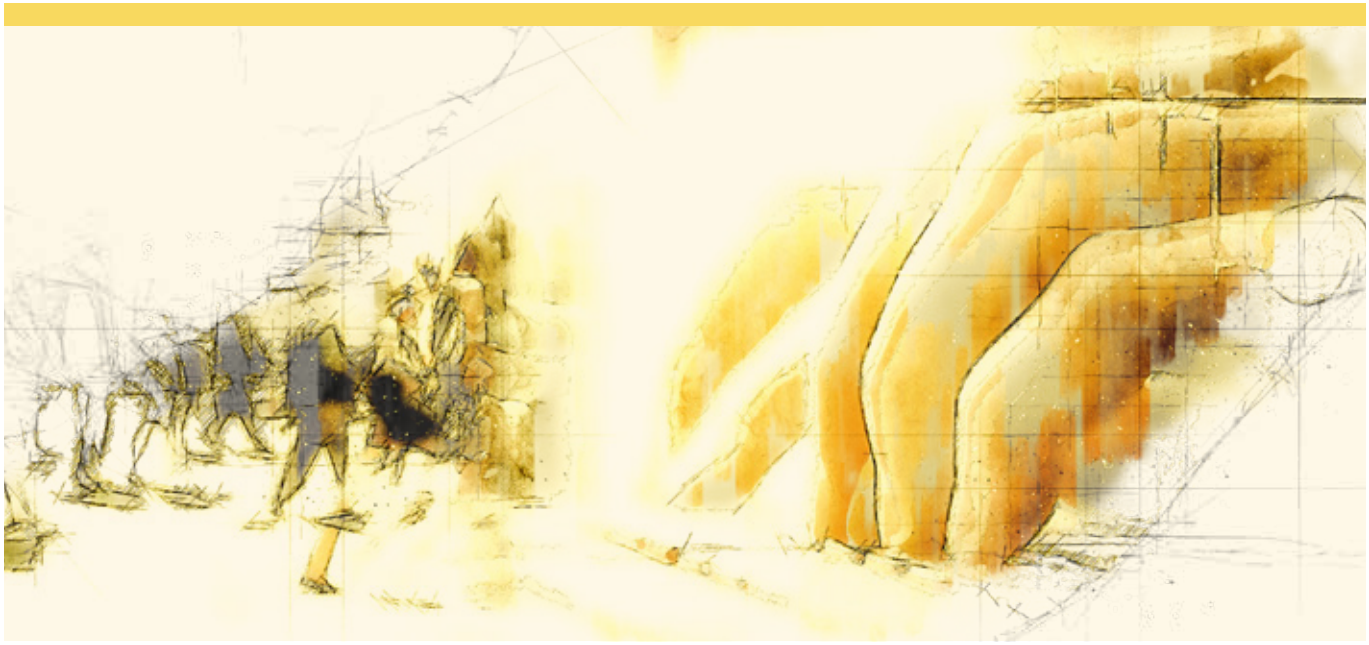
tet

Tilsynet med Efterretningstjenesterne



Årsredegørelse 2022

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 (TET) hermed redegørelse om sin virksomhed vedrørende Center for Cybersikkerhed (CFCS) for 2022. 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, juni 2023

Michael Kistrup
Formand for Tilsynet med Efterretningstjenesterne

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.

TET har i 2022 foretaget en omfattende og intensiv kontrol af CFCS, herunder af centrets behandling og videregivelse af data fra centrets sensornetværk, som danske myndigheder og virksomheder, der varetager samfundsvigtige funktioner, er tilkoblet.

CFCS har i forbindelse med gennemførelsen af TETs kontrol i 2022 generelt ydet en stor indsats for at bistå tilsynet ved deltagelse i møder, skriftlig forudgående afklaring af faktiske og retlige spørgsmål samt besvarelse af høringer vedrørende gennemførte kontroller.

TET og CFCS har løbende drøftelser om fortolkningen af CFCS-loven i relation til de forpligtelser, som er pålagt centret, samt tilsynets kontrol heraf. I overensstemmelse med det forudsatte i CFCS-loven inddrages forsvarsministeren i det omfang det er nødvendigt. Dette er blandt andet kommet til udtryk ved TETs kontrol af CFCS' behandlingssikkerhed i 2022.

I forhold til TETs øvrige virksomhed i 2022 har offentliggørelsen af tilsynets standarder for kontrol resulteret i øget national og international opmærksomhed og – på baggrund heraf – samarbejde og dialog med tilsvarende myndigheder og tænketanke i Danmark, Norden, Europa og Canada samt andre internationale organisationer. Hertil har TET i 2022 fortsat sit internationale samarbejde med andre nordiske og europæiske tilsynsmyndigheder, som udfører kontrol af efterretnings- og sikkerhedstjenester samt indledt et samarbejde med Det Uafhængige Tilsyn med Bevismidler (Bevismiddeltilsynet) om udveksling af medarbejdere i kortere perioder med henblik på sparring og gensidig kapacitetsopbygning.

Skala for TETs bemærkninger

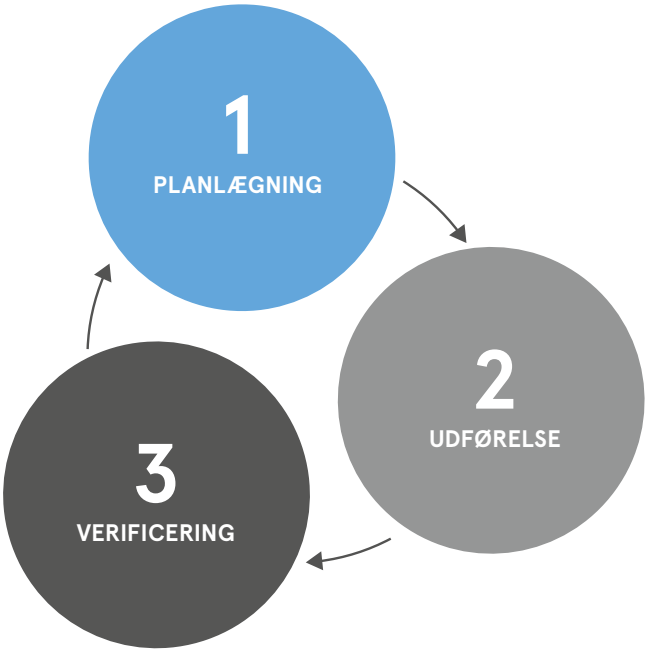
TETs bemærkninger tager udgangspunkt i følgende skala:

Bemærkninger	Baggrund for bemærkninger
»[...] **giver ikke anledning til bemærkninger**«	Anvendes når TET er enig med CFCS i, hvordan myndighederne generelt eller konkret administrerer loven.
»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 CFCS 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 egentlige lovbrud af et ikke uvæsentligt omfang 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 CFCS har udvist vilje til at sikre den fornødne afhjælpning heraf.

1. Kontrolmetode

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

Kontrollen af CFCS består overordnet af følgende delelementer:



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

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


GIN

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

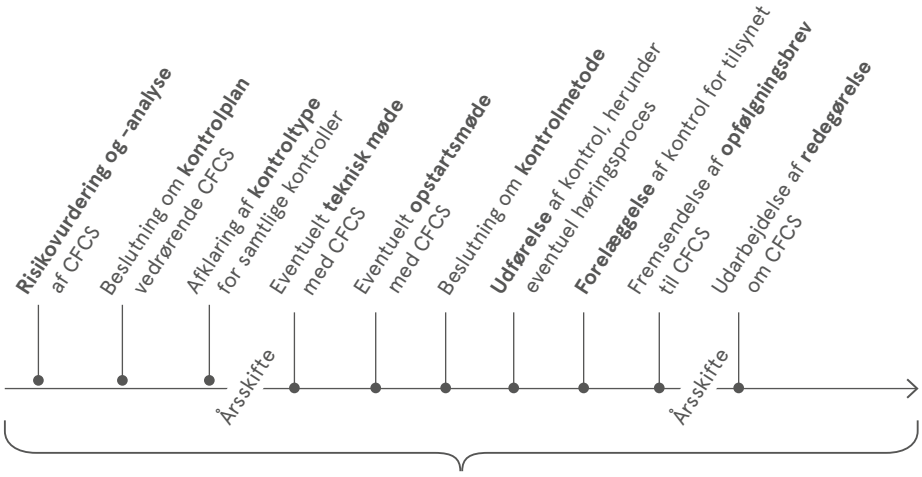
Kontrollen **2)** udføres løbende hen over året på baggrund af TETs beslutning om kontrolplan vedrørende CFCS. TET fastlægger ikke metoder for de enkelte kontroller i forbindelse med udarbejdelsen af risikovurderinger og -analyser, hvorfor metodevalget skal afklares forud for igangsættelse af en specifik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

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

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

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

TETs virksomhed forløber på følgende måde:



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

TETs direkte adgang til CFCS' systemer sikrer, at centret ikke kan forudse, hvilke sager og oplysninger der bliver genstand for kontrol. I nogle tilfælde er det imidlertid nødvendigt for TET 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.

TET deler forud for påbegyndelsen af årets kontroller sin risikoanalyse og kontrolplan med CFCS med henblik på at sikre åbenhed om tilsynets vurdering af forholdene i centret.

Åbenheden giver endvidere CFCS mulighed for at tage højde for TETs kontrol i tilrettelæggelsen af centrets interne kontrol, hvilket bidrager til, at tilsynets kontrol og centrets interne kontrol samlet dækker en større del af centrets virksomhed. Endelig sikrer åbenheden, at CFCS kan afsætte tilstrækkelige ressourcer til at betjene TET.

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

2. TETs kontrol

2.1 Sammenfatning af TETs kontrol i 2022

TET har i 2022 afsluttet 13 ud af 14 planlagte kontroller af CFCS.

Resultatet af TETs kontroller er beskrevet i deres helhed i afsnit 2.2. I det følgende fremhæves centrale og principielle dele af redegørelsen.

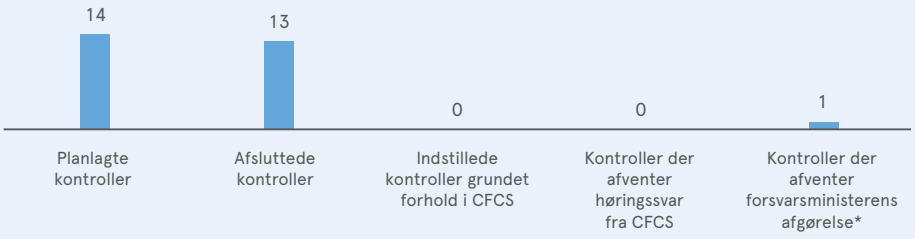
Det bemærkes, at nedenstående henvisninger alene udgør et mindre udsnit af TETs kontrol af CFCS i 2022. For det fulde billede af TETs kontrol af CFCS skal redegørelsen læses i sin helhed.

- 11 ud af 13 kontroller af CFCS gav ikke anledning til bemærkninger. Af de resterende to kontroller gav ingen anledning til bemærkninger om overordentligt kritisable eller kritisable forhold.

- TET konstaterede i én kontrol, at CFCS i tre tilfælde opbevarede oplysninger omfattet af CFCS-lovens kapitel 4, som burde være slettet, idet formålet med behandlingen var opfyldt, jf. CFCS-lovens § 17, stk. 1, samt at oplysningerne i tre tilfælde under alle omstændigheder burde være blevet slettet senest i august og september 2021, jf. CFCS-lovens § 17, stk. 2, nr. 1 (afsnit 2.2.3).

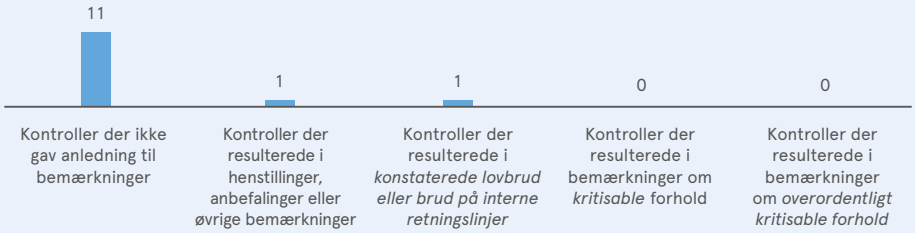
- TET fandt ikke, at det på baggrund af de foreliggende oplysninger var muligt at vurdere, om CFCS i to systemer havde truffet de fornødne sikkerhedsforanstaltninger i henhold til CFCS-lovens § 18 (afsnit 2.2.7).

TETs kontrol af CFCS i 2022



* Se afsnit 2.2.10

Resultater af TETs kontrol af CFCS i 2022



Note: Såfremt en kontrol har haft flere forskellige resultater, eksempelvis både henstillinger, konstateringer af lovbrud og bemærkninger om kritisable eller overordentligt kritisable forhold, vil disse tælle med under hver kategori.

2.2 Gennemførte kontroller af CFCS i 2022

Med henblik på at kontrollere at CFCS i forbindelse med behandling af oplysninger om fysiske personer overholder reglerne i CFCS-loven, har TET i 2022 foretaget kontrol af centrets

- behandling af oplysninger på sensornetværk (2.2.1),
- behandling af oplysninger i separate it-miljøer og analyseværktøjer (2.2.2),
- behandling af oplysninger i andre systemer (2.2.3),
- anvendelse af edition (2.2.4),
- videregivelse af oplysninger til andre myndigheder, virksomheder og samarbejdspartnere (2.2.5),
- udveksling af oplysninger med den øvrige del af FE (2.2.6),
- behandlingssikkerhed (2.2.7),
- interne kontrol (2.2.8) og
- opfølgning på TETs kontroller i 2021 (2.2.9).

Endvidere har TET i 2022 gennemført

- tekniske undersøgelser og kortlægning af CFCS' it-landskab (2.2.10).

2.2.1 Kontrol af CFCS' behandling af oplysninger på sensornetværk

CFCS driver et sensornetværk, som overvåger internettrafik hos tilsluttede myndigheder og virksomheder (såkaldte NSS-sensorer). Sensorerne indeholder en række regler, der bruges til at genkende forsøg på cyberangreb. Når der via sensorerne registreres potentielt ondsindet trafik, som passer på en regel, modtager CFCS en alarm. Medarbejdere i CFCS henter derefter et relevant udsnit af internettrafikken med henblik på at foretage en undersøgelse af årsagen hertil.

Foruden NSS-sensorerne driver CFCS et sensornetværk med henblik på at skabe et nationalt situationsbillede, der kan danne grundlag for centrets varsling om observerede trusler (såkaldte NCSO-sensorer).

Data indhentet fra CFCS' sensornetværk, må højst opbevares i enten 5 år, 3 år eller 13 måneder, jf. CFCS-lovens § 17, stk. 2, nr. 1-3. Hvor længe CFCS må opbevare sensordata afgøres af, om data knytter sig til en sikkerhedshændelse, samt om der er tale om sensordata fra myndigheder, som særligt beskæftiger sig med eller har særlig betydning for udenrigs-, sikkerheds- og forsvarspolitiske forhold, samt virksomheder og organisationer, hvis aktiviteter har særlig betydning for disse forhold.

TET har i 2022 foretaget kontrol af CFCS' behandling, herunder sletning, af oplysninger på begge sensornetværk.

TETs bemærkninger

TETs kontrol af CFCS' anvendelse af centrets sensornetværk gav ikke anledning til bemærkninger.

2.2.2 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 lagrer 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 har i 2022 foretaget kontrol af CFCS' behandling af oplysninger i to analyseværktøjer.

TETs bemærkninger

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

2.2.3 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, fildrev eller mailsystemer.

Behandlingen kan både omfatte almindelige personoplysninger, samt oplysninger, der stammer fra indgreb i meddelelseshemmeligheden i henhold til CFCS-lovens kapitel 4, eksempelvis oplysninger fra centrets sensornetværk.

TET har i 2022 foretaget kontrol af CFCS' behandling af oplysninger i andre systemer ved

- kontrol af et filsystem,
- kontrol af et fællesdrev og
- kontrol af arbejdsstationer i CFCS.

TETs bemærkninger

TET konstaterede, at CFCS i tre tilfælde opbevarede oplysninger omfattet af CFCS-lovens kapitel 4, som burde være slettet, idet formålet med behandlingen var opfyldt, jf. CFCS-lovens § 17, stk. 1, samt at oplysningerne i tre tilfælde under alle omstændigheder burde være blevet slettet senest i august og september 2021, jf. CFCS-lovens § 17, stk. 2, nr. 1. Oplysningerne var slettet fra den brugerrettede del af systemet, men kunne fortsat tilgås af CFCS' systemadministratorer.

Fristen for sletning i henhold CFCS-lovens § 17, stk. 2, nr. 1, blev ved lov nr. 555 af 7. maj 2019 (lov om ændring af lov om Center for Cybersikkerhed) forlænget fra 3 til 5 år. Idet de pågældende oplysninger var tilvejebragt før 1. juli 2019, var det imidlertid den tidligere slettefrist på 3 år, som var gældende for oplysningerne, jf. ændringslovens § 2, stk. 2.

Forsvarsministeren traf den 1. november 2021 afgørelse vedrørende anvendelsesområdet for CFCS-lovens § 17, stk. 1, i forhold til sensordata på baggrund af TETs kontrol af centrets

sensornetværk i 2019 (se tilsynets redegørelse for 2021, afsnit 2). TET oplyste i forbindelse med kontrollen af arbejdsstationer i 2022, at det er tilsynets opfattelse, at centret er forpligtet til at slette sensordata, som behandles på medarbejderes arbejdsstationer, når formålet med behandlingen er opfyldt, jf. CFCS-lovens § 17, stk. 1, idet forsvarsministerens afgørelse efter tilsynets opfattelse alene vedrører sensordata, som opbevares centralt.

CFCS oplyste, at det er centrets opfattelse, at forsvarsministerens afgørelse tillige er gældende for centrets behandling af sensordata på arbejdsstationer, da det fremgår af ministerens afgørelse af 1. november 2021, at CFCS-lovens § 17, stk. 1, i forhold til sensordata har et meget begrænset anvendelsesområde, og at bestemmelsens primære anvendelsesområde er de øvrige former for data, der er omfattet af CFCS-lovens kapitel 4. CFCS vil på den baggrund forelægge sagen for forsvarsministeren til afgørelse.

2.2.4 Kontrol af CFCS' anvendelse af edition

Edition er en særlig lovhjemmel i CFCS-lovens kapitel 4 a, som gør det muligt at pålægge tredjeparter at udlevere oplysninger til CFCS om brugeren af en e-mailadresse, IP-adresse eller et domænenavn. Pålægget forudsætter, at CFCS forinden har indhentet en retskendelse som grundlag for editionen.

Ved editionen pålægger retten den person, som har rådighed over oplysningerne, typisk en teleudbyder, at udlevere disse til CFCS.

TET har i 2022 foretaget kontrol af CFCS' anvendelse af edition.

TETs bemærkninger

TETs kontrol af CFCS' anvendelse af edition gav ikke anledning til bemærkninger.

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

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

TET har i 2022 foretaget kontrol af CFCS' videregivelse af oplysninger.

TETs bemærkninger

TETs kontrol af CFCS' videregivelse af oplysninger gav ikke anledning til bemærkninger.

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

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

TET har i 2022 foretaget kontrol af CFCS' udveksling af oplysninger med den øvrige del af FE. Kontrollen har særligt været fokuseret på, om CFCS' har sikret den tilstrækkelige adgangsbegrænsning af informationssystemer, hvor der behandles oplysninger der stammer fra indgreb i meddelelseshemmeligheden, jf. CFCS-cirkulærets § 4.

TETs bemærkninger

TETs kontrol af CFCS' udveksling af oplysninger, der stammer fra indgreb i meddelelseshemmeligheden, med den øvrige del af FE, gav ikke anledning til bemærkninger.

2.2.7 Kontrol CFCS' overholdelse af reglerne om behandlingssikkerhed

CFCS er i henhold til CFCS-lovens § 18 forpligtet til at træffe 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.

TET har i forhold til to kontroller i 2022 stillet uddybende spørgsmål om, hvordan CFCS sikrer at behandling af oplysninger i de pågældende systemer sker i overensstemmelse med kravene i CFCS-lovens § 18.

TET har i den forbindelse anmodet CFCS om at oplyse:

- Hvilke foranstaltninger CFCS har iværksat for at sikre, at behandling af oplysninger i systemerne sker i overensstemmelse med CFCS-lovens § 18.
- Hvorvidt CFCS har foretaget en risikovurdering af behandlingssikkerheden for oplysninger, som behandles i systemerne.

CFCS har henvist til centrets initiativer på ISO 27001-området vedrørende behandlingssikkerhed samt Statsministeriets sikkerhedscirkulære nr. 10338 af 17. december 2014 og de militære sikkerhedsbestemmelser (FKOBST 358-1), der også indeholder en række krav til behandlingssikkerhed, som dokumentation for, hvilke foranstaltninger centret blandt andet har iværksat for at sikre behandlingssikkerhedsniveauet.

CFCS har desuden oplyst, at centret ikke mener, at CFCS-lovens § 18 indeholder en retlig forpligtelse for centret til at foretage risikovurderinger på systemniveau ved etableringen af systemer inden for den eksisterende it-infrastruktur.

TETs bemærkninger

TET oplyste, at tilsynet ikke er enig i CFCS' vurdering af, at det ikke har været hensigten med CFCS-lovens § 18, at fastsætte konkrete retlige krav til centrets behandlingssikkerhed.

Endvidere oplyste TET, at det er tilsynets vurdering, at CFCS-lovens § 18 – ligesom den tidligere gældende § 41, stk. 3, i persondataloven – konkret forpligter CFCS til at træffe de fornødne tekniske og organisatoriske forholdsregler, som sikrer mod de i bestemmelsen beskrevne risici. Det fremgår af de særlige bemærkninger til persondatalovens § 41, stk. 3, at det forudsættes, at foranstaltningerne under hensyn til det aktuelle tekniske niveau og de omkostninger, som er forbundet med deres iværksættelse, vil tilvejebringe et tilstrækkeligt sikkerhedsniveau i forhold til de risici, som behandlingen indebærer, og arten af de oplysninger som skal beskyttes.

TET vurderede på den baggrund, at CFCS i de tilfælde, hvor centret foretager behandling af oplysninger, er forpligtet til at foretage en vurdering af, hvilke foranstaltninger der kan tilvejebringe et tilstrækkeligt sikkerhedsniveau. Vurderingen vil skulle tage højde for de risici, som behandlingen indebærer, og arten af de oplysninger som skal beskyttes, under hensyntagen til det aktuelle tekniske niveau og de omkostninger, som er forbundet med deres iværksættelse. Når CFCS har gennemført vurderingen, vil centret herefter være forpligtet til at sikre, at de pågældende foranstaltninger bliver implementeret for den pågældende behandling.

TET vurderede, at det er en forudsætning for tilsynets kontrol af CFCS' overholdelse af CFCS-lovens § 18, at centret dokumenterer sin vurdering af, hvilke foranstaltninger centret finder nødvendige at implementere med henblik tilvejebringe et tilstrækkeligt sikkerhedsniveau i forhold til de risici, som behandlingen indebærer, og arten af de oplysninger som skal beskyttes.

TET fandt ikke, at det på baggrund af de foreliggende oplysninger var muligt at vurdere, om CFCS i de to systemer havde truffet de fornødne sikkerhedsforanstaltninger i henhold til CFCS-lovens § 18.

CFCS oplyste efter kontrollen, at centrets besvarelse skal forstås sådan, at de tiltag, som er implementeret på tværs af systemporteføljen, efter centrets vurdering generelt kan antages at leve op til kravene i CFCS-lovens § 18.

CFCS oplyste på baggrund af kontrollen, at centret er uenig i TETs vurdering, hvorfor centret vil forelægge sagen for forsvarsministeren til afgørelse.

CFCS' overholdelse af reglerne om behandlingssikkerhed vil fortsat være et fokuspunkt for TET.

2.2.8 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.

CFCS har i maj 2022 orienteret TET om centrets

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

CFCS har derudover løbende orienteret TET om centrets interne kontrol.

TETs bemærkninger

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

2.2.9 Opfølgning på TETs kontrol af CFCS i 2021

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 har i 2022 foretaget opfølgning på tilsynets kontrol af CFCS i 2021.

TETs bemærkninger

TETs opfølgning på kontrollen af CFCS i 2021 gav ikke anledning til bemærkninger.

2.2.10 TETs tekniske undersøgelser og kortlægning

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 2022 gennemgået og verificeret omfattende dele af CFCS' it-landskab, og arbejder løbende med at sikre et ajourført 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.

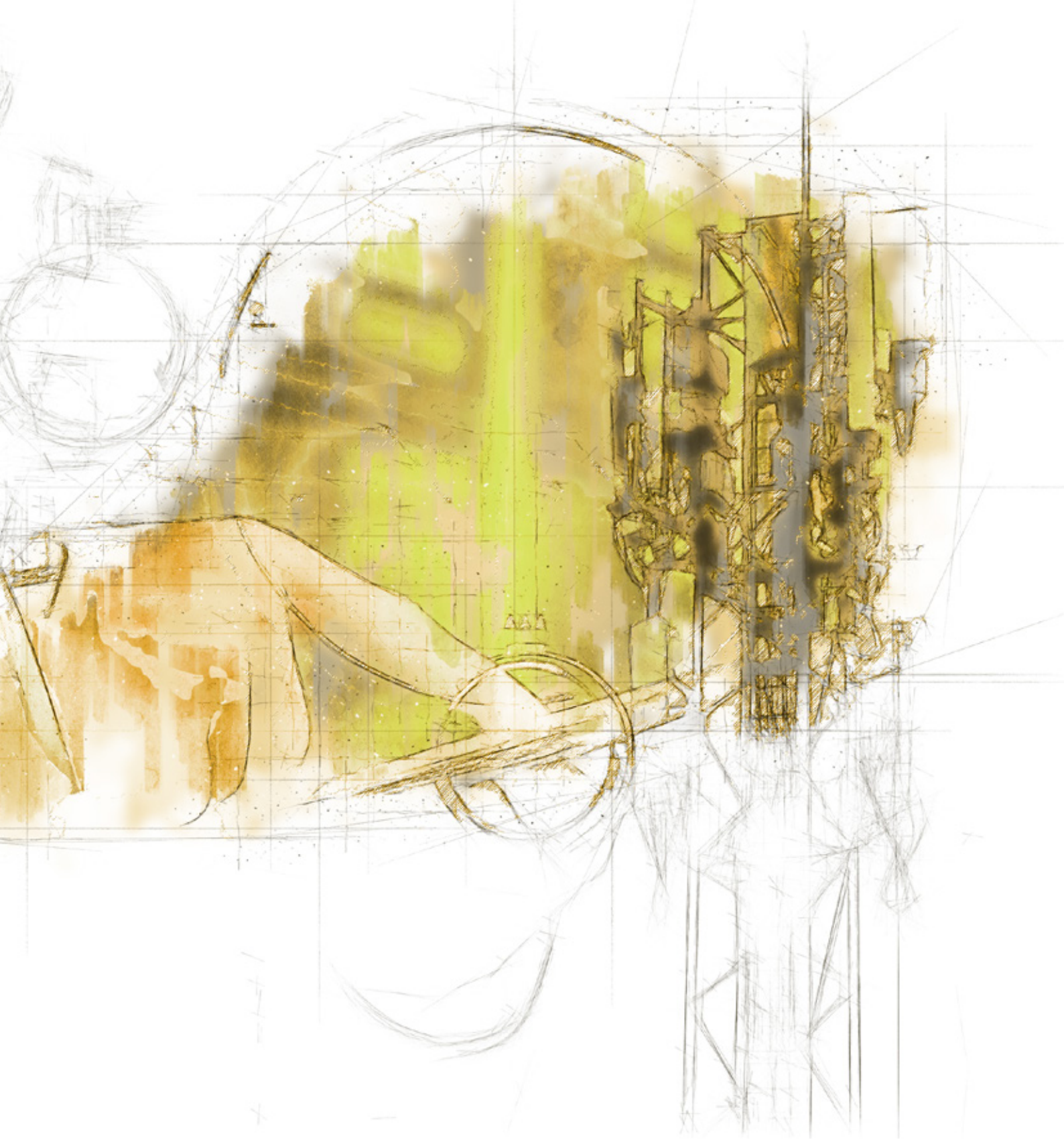
TET har i 2022 foretaget valideringskontroller og inspektioner af CFCS' it-infrastruktur ved inspektion af et antal systemer, som tilsynet umiddelbart vurderede ikke skulle være en del af tilsynets almindelige kontroller, med henblik på at afdække om den umiddelbare vurdering heraf var retvisende.

TET har i 2022 tillige igangsat en kortlægning af CFCS' håndtering af sletning af data fra centrets sensornetværk. Kortlægningen forventes færdiggjort i løbet af 2023.

2.3 CFCS' sagsbehandlingstider i 2022

TETs har i 2022 fremsendt syv juridiske høringer til CFCS i forbindelse med tilsynets kontrolvirksomhed. CFCS har besvaret 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 30 arbejdsdage.

TET har i 2022 været i dialog med CFCS og udarbejdet en ny proces for behandling af høringer.



3. 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 2022:

CFCS har til opgave at beskytte de vigtige dele af det danske samfund mod cyberangreb. I praksis løses denne opgave ved, at Netsikkerhedstjenesten 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. Netsikkerhedstjenesten består af flere organisatoriske enheder i CFCS.

I 2022 har Netsikkerhedstjenesten håndteret en lang række sikkerhedshændelser for myndigheder og virksomheder i og uden for sensornetværket. Størstedelen af disse hændelser omhandlede rekognoscering, social engineering og kompromitteringer i form af dataspionage og datatyveri. CFCS har observeret angreb og forsøg på angreb fra både statsstøttede og kriminelle cyberaktører også i 2022.

Baseret på CFCS' observationer anses angrebsforsøg via phishing fortsat som 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 forskellige typer forsøg på at udnytte fejlkonfigurationer og sårbarheder i softwaretjenester, som er eksponeret mod internettet. Det omfatter også brute force-relaterede angrebsforsøg rettet mod eksponerede it-systemer, som angriberen forsøger at tvinge sig adgang til.

4. 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 2022:

TABEL 1

Videregivelser og udvekslinger

Kategorier	2022
Videregivelser	46
Udvekslinger	6

TABEL 2

Sikkerhedshændelser* efter alvorlighedsgrad

Kategorier	2022
Alvorlige cyberangreb	3
Større cyberangreb	2
Moderate cyberangreb	23
Mindre cyberangreb	328
Ingen/begrænset effekt**	1.468
Falske positive***	1.253
Total	**3.077**

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

TABEL 3

Aktindsigtssager

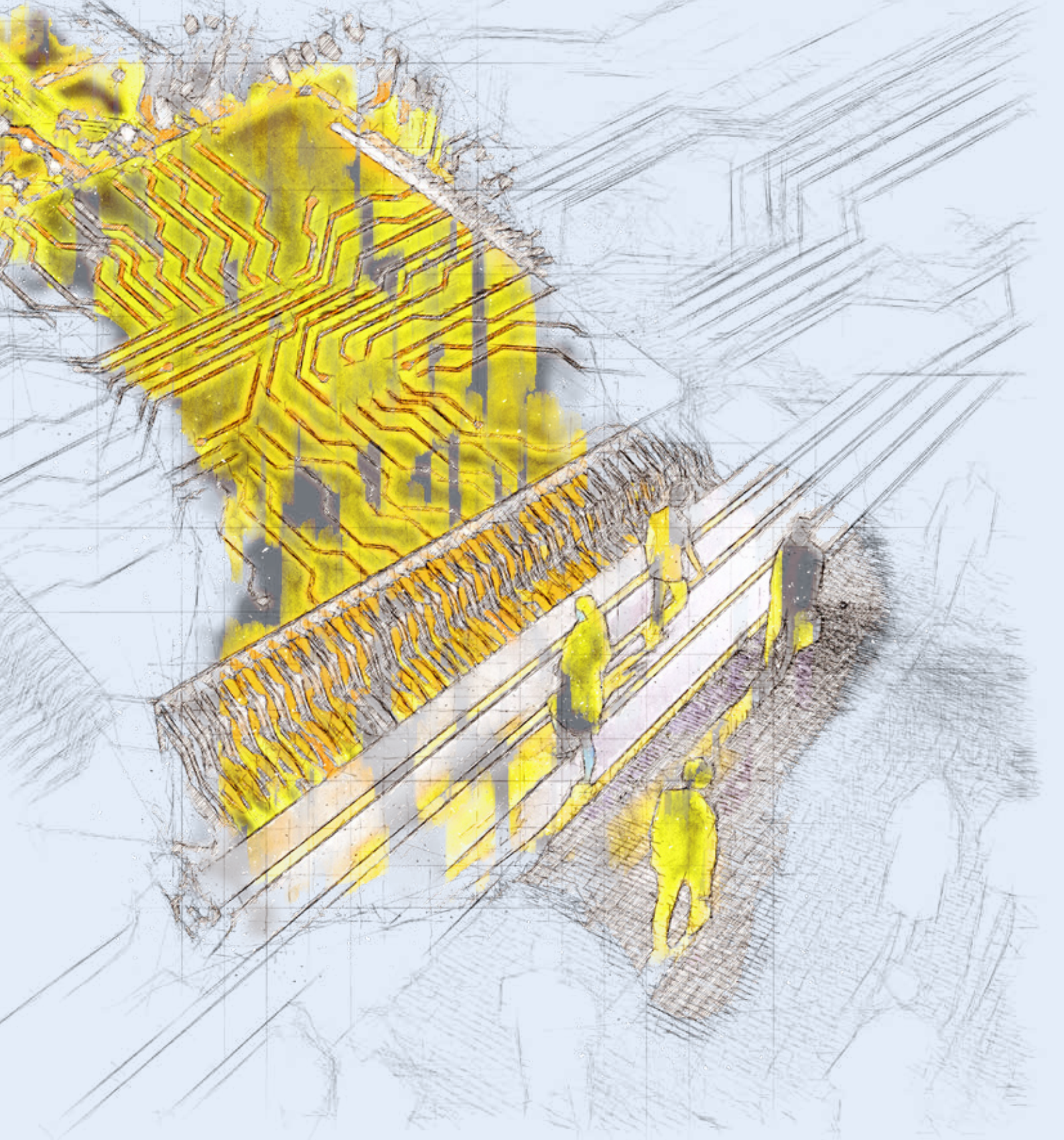
Kategorier	2022
Fuld aktindsigt	3
Delvis aktindsigt	1
Afslag på aktindsigt	6
Ingen omfattede dokumenter lokaliseret	0
Total	**10**

TABEL 4

Behandling af personoplysninger

Kategorier	2022
Klager til CFCS over behandling af personoplysninger	0*
Klagesager modtaget i TET	0

* CFCS har ikke kendskab til at der er modtaget klager



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.

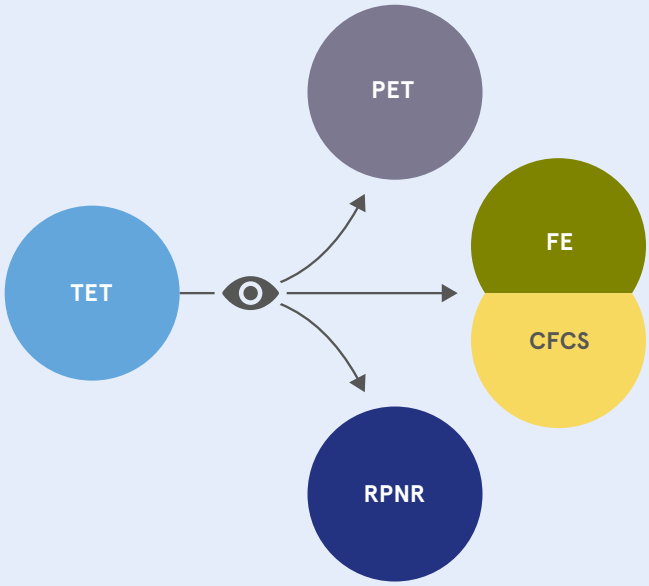
Appendiks

2. Tilsynet med Efterretningstjenesterne

TETs virksomhed

Personale i 2022 (ansatte)	8
Finanslovsbevilling i 2022 (mio. kr.)	9,9

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



TET udøver sine funktioner i fuld uafhængighed og er således ikke undergivet tjeneste-befalinger fra 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 2022:

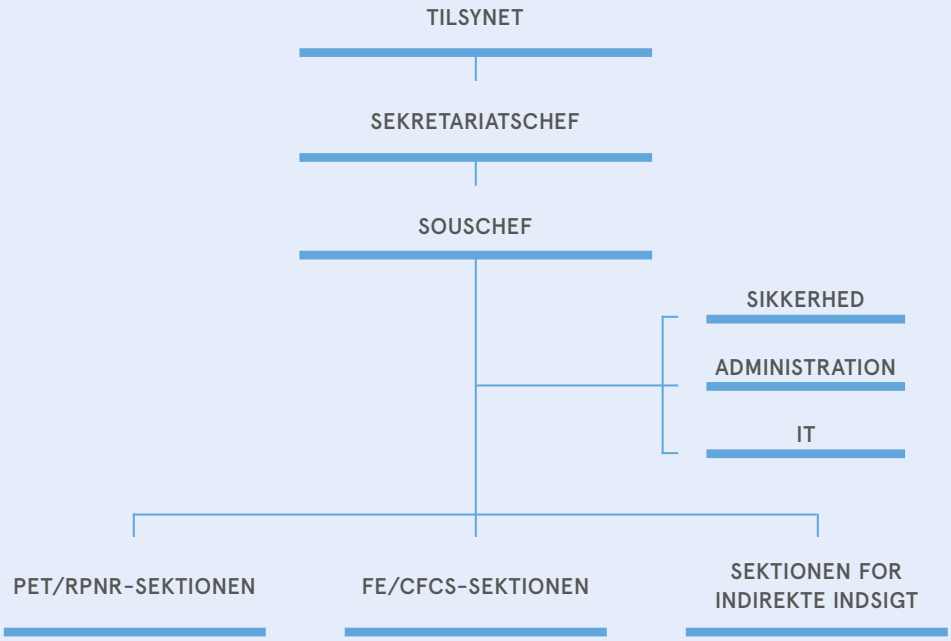
- Landsdommer Michael Kistrup, Østre Landsret (formand)
- Juridisk chef Pernille Christensen, Kommunernes Landsforening
- Professor Henrik Udsen, Københavns Universitet
- Professor Rebecca Adler-Nissen, Københavns Universitet
- Direktør Jesper Fisker, Kræftens Bekæmpelse

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

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 2022 bestod sekretariatet af en sekretariatschef, der varetager den daglige ledelse, en souschef, tre jurister, to it-konsulenter og en kontorfunktionær.

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

Organisation 2022



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

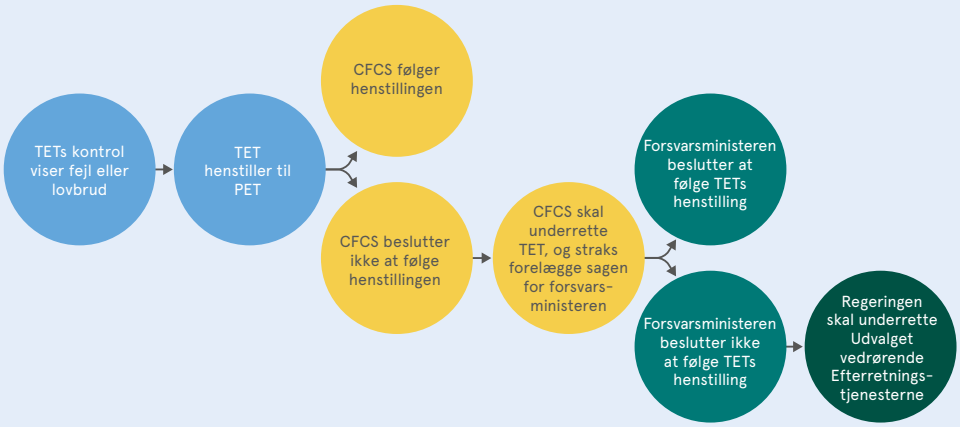
TET kan hos CFCS kræve enhver oplysning og alt materiale, der er af betydning for tilsynets virksomhed, og har til enhver tid adgang til alle lokaler, hvorfra der er adgang til de oplysninger, som behandles, eller hvor tekniske hjælpemidler anvendes. TET kan endvidere afkræve CFCS skriftlige udtalelser 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 personoplysninger. Hvis CFCS undtagelsesvis måtte beslutte ikke at følge en henstilling i en udtalelse fra TET, skal centret underrette tilsynet herom og straks forelægge sagen for forsvarsministeren til afgørelse.

TETs reaktionsmuligheder



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 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 TET 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. 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 maj 2022. Redegørelsen blev offentliggjort i juni 2022.

Appendiks 3. Retsgrundlag

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

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

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

3.1 CFCS' netsikkerhedstjeneste

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

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

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

3.2 Indgreb i meddelelseshemmeligheden og edition

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

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

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

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

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

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

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

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

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

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

3.2.2 Om edition, jf. CFCS-lovens § 7

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

3.3 Behandling af personoplysninger

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

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

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

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

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

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

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

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

6) behandlingen er nødvendig for, at CFCS eller den tredjemand, til hvem oplysningerne

videregives, kan forfølge en berettiget interesse, og hensynet til den pågældende person ikke overstiger denne interesse, eller

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

4) Som led i det løbende arbejde med at understøtte et højt informationssikkerhedsniveau på Forsvarsministeriets område, herunder ved kontrol af om kommunikation

indeholder klassificeret materiale, kan trafikdata og pakkedata, der hidrører fra myndigheder på Forsvarsministeriets område, analyseres.

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

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

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

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

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

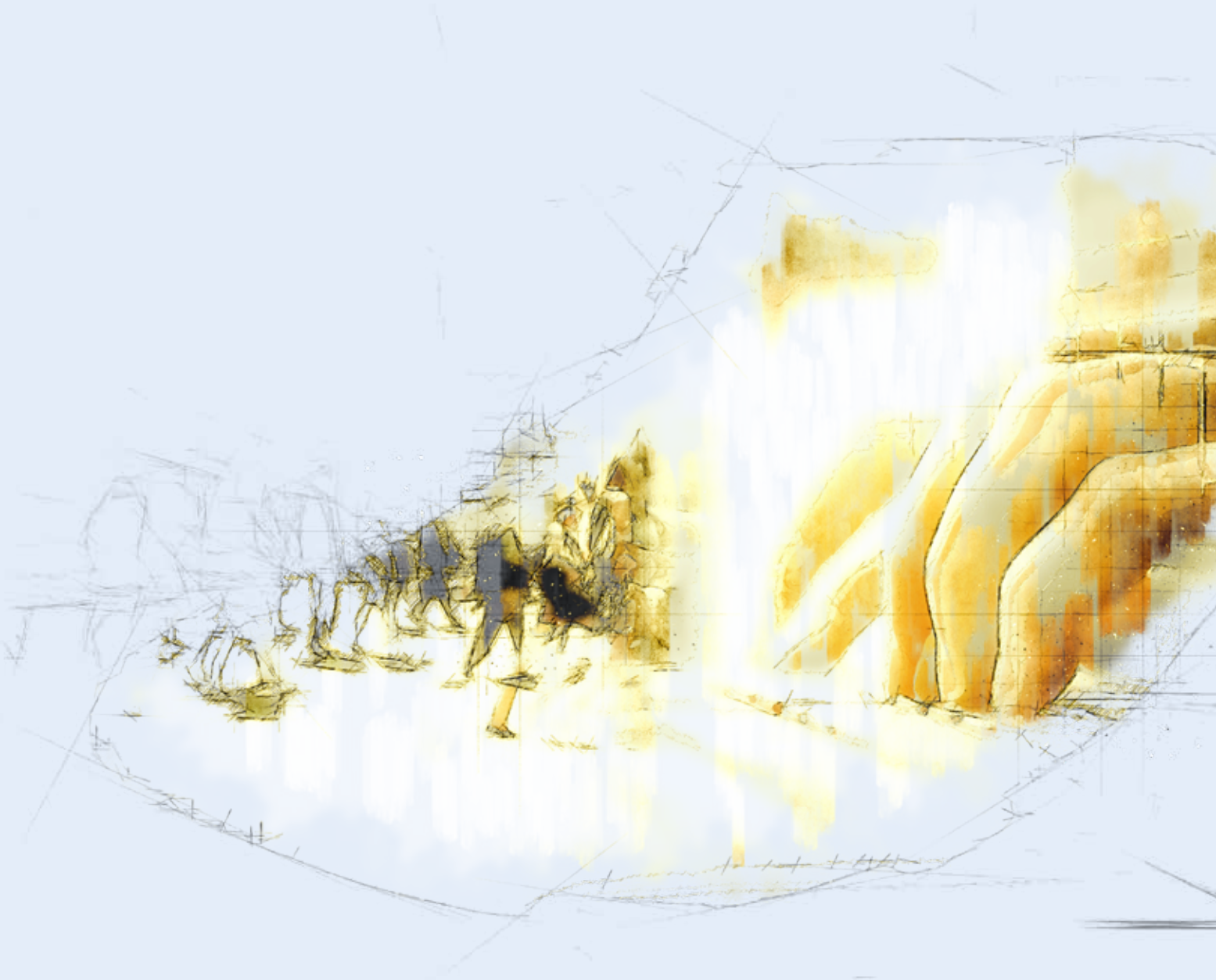
1) data, der knytter sig til en sikkerhedshændelse, højst opbevares i fem år,

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

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

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

Forsvarsministeren har i 2021 – på baggrund af 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 udenrigs-efterretningstjeneste kan bidrage med en række værdifulde oplysninger.

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

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

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

3) der er begrundet mistanke om en sikkerhedshændelse.

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

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

Årsredegørelse 2022
Center for Cybersikkerhed
Udgivet af Tilsynet med Efterretningstjenesterne, juni 2023
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