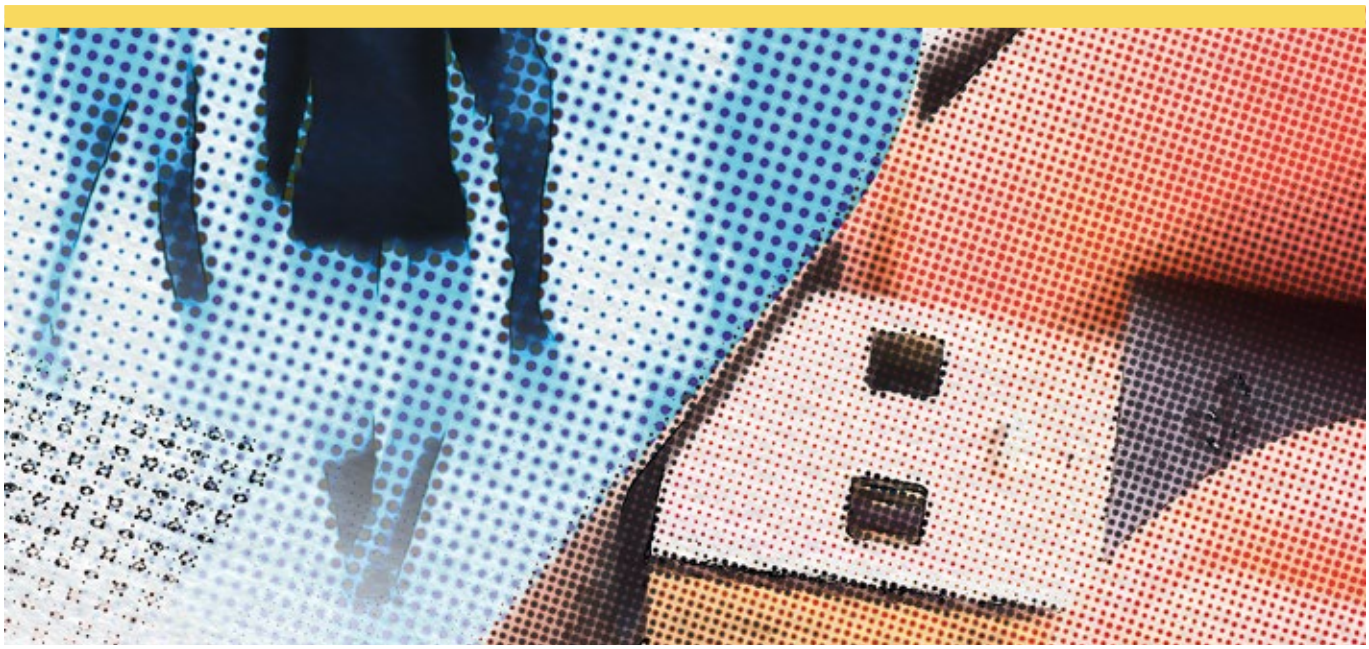
Tilsynet med Efterretningstjenesterne



Årsredegørelse 2018

Center for Cybersikkerhed

Indhold

Til forsvarsministeren

I overensstemmelse med § 24 i lov om Center for Cybersikkerhed (lov nr. 713 af 25. juni 2014, som senest ændret ved lov nr. 555 af 7. maj 2019) afgiver Tilsynet med Efterretningstjenesterne hermed redegørelse om sin virksomhed vedrørende Center for Cybersikkerhed for 2018. Redegørelsen skal offentliggøres.

København, juni 2019

Michael Kistrup

Formand for Tilsynet med Efterretningstjenesterne

Forord

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

Sigtet med nærværende redegørelse er at informere om karakteren af det tilsyn, der udøves vedrørende CFCS. Redegørelsen indeholder oplysninger om de forhold, som tilsynet i 2018 har valgt særligt at interessere sig for, og om i hvor mange tilfælde tilsynet har fundet, at centrets behandling af personoplysninger ikke har været i overensstemmelse med reglerne. Endvidere indeholder redegørelsen i relevant omfang opfølgning på tilsynets kontroller i 2016 og 2017.

Som i de forgangne år har tilsynet i 2018 haft fokus på at konsolidere og styrke grundlaget for tilsynets kontrol af henholdsvis CFCS, Forsvarets Efterretningstjeneste (FE) og PET, herunder ved løbende udvikling af tilsynets risiko- og væsentlighedsvurdering af tjenesterne og centret samt de standarder og metoder, som anvendes i den retlige kontrol heraf. Det er afgørende for tilsynet, at de enkelte kontroller er velunderbyggede og -dokumenterede, og at de er tilrettelagt på baggrund af en tilstrækkelig efterretningsfaglig og teknisk forståelse. Tilsynet har endvidere i 2018 igangsat flere udviklingsprojekter med henblik på at sikre en mere effektiv systemunderstøttelse af tilsynets kontrolvirksomhed.

Tilsynet har i 2018 gennemført en omfattende og intensiv kontrol med CFCS' behandling af oplysninger om fysiske personer. Som i de foregående år har tilsynet prioriteret kontroller med fokus på CFCS' overholdelse af reglerne om indgreb i meddelelseshemmeligheden, behandling af personoplysninger samt analyse, videregivelse og sletning af data.

Tilsynet har herudover prioriteret kontrol af CFCS' overholdelse af reglerne om sikkerhedsforanstaltninger (informationssikkerhed) i forbindelse med behandling af personoplysninger. Mens reglerne om sikkerhedsforanstaltninger er et fokusområde i samtlige af tilsynets kontroller af centret, håndteres implementeringen af ISO 27001-standarden i et samlet projekt for FE og CFCS. Tilsynets kontrol heraf er behandlet nærmere i redegørelsen om FE for 2018, afsnit 1.2.12. Endelig har tilsynet fortsat sit arbejde med kortlægning og verificering af CFCS' systemlandskab på server- og komponentniveau.

Tilsynet har i 2018 udbygget sit samarbejde med hollandske Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD), belgiske Comité permanent de contrôle de services de renseignements et de sécurité (Committee I), norske Stortingets Kontrollutvalg for etterretnings-, overvåknings- og sikkerhetstjeneste (EOS-utvalget) samt schweiziske Unabhängige Aufsichtsbehörde über die nachrichtendienstlichen Tätigkeiten (AB-ND). Fokus i dette samarbejde er erfaringsudveksling omkring kontrolmetoder samt drøftelse af juridiske emner af fælles relevans. Samarbejdet har blandt andet resulteret i, at de fem tilsynsmyndigheder i november 2018 offentliggjorde en fælles udtalelse om styrkelse af samarbejdet mellem nationale tilsyn med efterretningstjenester. Udtalelsen kan findes på tilsynets hjemmeside.

Tilsynets sekretariat har tillige i april 2018 besøgt de svenske tilsynsmyndigheder Säkerhets- och integritetsskyddsnämnden (SIN) og Statens inspektion för försvarsunderrättelseverksamheten (SIUN), hvor tilsynet udvekslede erfaringer om forskellige kontrolmetoder.

Foruden tilsynets tætte samarbejde med udvalgte tilsynsmyndigheder deltog tilsynet i december 2018 i en fælles europæisk konference for tilsynsmyndigheder i Paris, hvor 14 europæiske lande deltog.

Michael Kistrup

Formand for Tilsynet med Efterretningstjenesterne

1 Tilsynets kontrol

1.1 Kontrolmetode

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

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

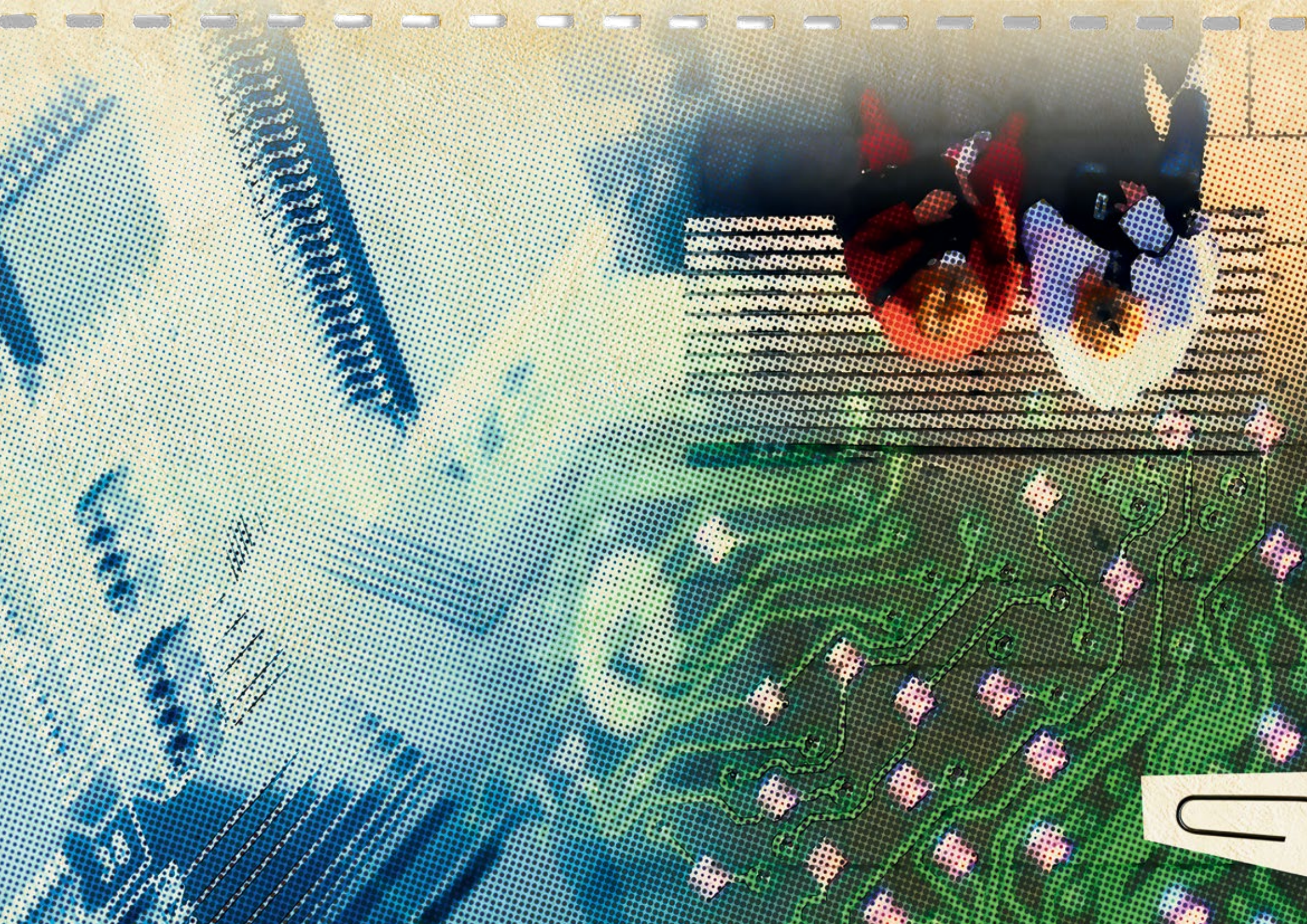
Tilsynets planlægning af kontrollerne for det kommende år sker på baggrund af en årlig risikovurdering vedrørende samtlige processer og systemer hos CFCS. Formålet med risikovurderingen er at vurdere risici for lovbrud i relation til indgreb i meddelelseshemmeligheden, behandling, analyse, videregivelse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

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

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

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

Tilsynet benytter sig af en række forskellige metoder i kontrollen af de enkelte områder, heriblandt fuldstændig kontrol, stikprøvekontrol, indholdsscreening og interviewbaseret



kontrol. Tilsynets valg af metode sker på baggrund af risikoanalysen af området, erfaringer fra tidligere kontroller og de faktiske forhold, som tilsynet konstaterer i forbindelse med kontrollen. Endvidere afholder tilsynet forud for kontrol af ikke tidligere kontrollerede områder et opstartsmøde med de relevante medarbejdere i CFCS med henblik på at sikre en tilstrækkelig teknisk forståelse af området, således at kontrollen kan tilpasses og gennemføres hensigtsmæssigt.

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

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

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

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

1.2 Kontrol af CFCS i 2018

Med henblik på at kontrollere at CFCS i forbindelse med behandling af oplysninger om fysiske personer overholder reglerne i CFCS-loven, har tilsynet i 2018 foretaget kontrol af centrets

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

Sammenfatning af tilsynets kontroller i 2018

Tilsynets kontroller vedrørende CFCS' iagttagelse af bestemmelserne om indgreb i meddelelseshemmeligheden, behandling af personoplysninger, analyse, videregivelse og sletning af data viste, jf. afsnit. 1.2.1-1.2.3 og 1.2.5, at centret generelt har overholdt lovgivningens bestemmelser herom.

Tilsynets kontrol vedrørende CFCS' behandling af oplysninger i relation til indleverede medier viste imidlertid, jf. afsnit 1.2.2, at centret på tidspunktet for tilsynets første inspektionsbesøg ikke iagttog lovgivningens krav til sikkerhedsforanstaltninger i CFCS-lovens § 18, stk. 1. Kontrollen viste tillige, at centrets interne retningslinjer indeholdt procedurer, som ikke var i overensstemmelse med CFCS-lovens bestemmelser. På tidspunktet for tilsynets andet inspektionsbesøg havde CFCS imidlertid iværksat en række tiltag, med henblik på at sikre at behandlingen af oplysninger i relation til indleverede medier finder sted i overensstemmelse med CFCS-lovens § 18, stk. 1, herunder revideret sine interne retningslinjer for behandling af indleverede medier.

Tilsynets kontrol vedrørende CFCS' udveksling af data indeholdende personoplysninger, der stammer fra indgreb i meddelelseshemmeligheden, med den øvrige del af FE viste, jf. afsnit 1.2.4, at centrets udvekslinger er sket under iagttagelse af Forsvarsministeriets retningslinjer vedrørende behandling af data i og fra Center for Cybersikkerheds netsikkerhedstjenestes (CFCS-retningslinjerne) bestemmelser herom, men at der i ét tilfælde ikke forelå forudgående juridisk godkendelse heraf som foreskrevet i centrets interne retningslinjer. På baggrund af kontrollen opfordrede tilsynet CFCS til at sikre en ensrettet dokumentation og registrering af centrets udvekslinger, herunder med henblik på at kunne foretage en effektiv kontrol heraf.

Kontrollen af CFCS' interne kontrol viste, jf. afsnit 1.2.6, at centrets interne kontrol i 2018 – som adviseret i 2016 og 2017 – ikke har været tilrettelagt på baggrund af en dokumenteret og ledelsesgodkendt risiko- og væsentlighedsvurdering. Sammenholdt med manglende afrapportering vedrørende CFCS' interne kontroller i 2018 har tilsynet på det grundlag, som forelå på tidspunktet for afslutningen af kontrollen, ikke kunnet vurdere, hvorvidt CFCS' interne kontrol i 2018 har været tilfredsstillende. Tilsynet noterer sig imidlertid, at CFCS efterfølgende har fremsendt en dokumenteret og ledelsesgodkendt risiko- og væsentlighedsvurdering samt afrapportering på afviklede interne kontroller i 2018.

1.2.1 Kontrol af CFCS' anvendelse af analyseværktøjer

CFCS anvender en række forskellige analyseværktøjer i forbindelse med analyse af data fra henholdsvis centrets sensornet og medier, som indleveres til centret. CFCS' analyse tilpasses løbende de trusler, som centret bliver opmærksom på i forbindelse med sin virksomhed, hvorfor der konstant sker ændringer i, hvilke analyseværktøjer der er relevante at anvende.

Med henblik på kontrol heraf havde tilsynet i 2018 løbende drøftelser med CFCS om centrets anvendelse af analyseværktøjer.

! **Tilsynets bemærkninger**

Tilsynet har på baggrund af centrets redegørelse afsluttet kontrollen af analyseværktøjer i 2018 og igangsat yderligere kontrol af området i 2019.

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

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

Med henblik på kontrol af CFCS' behandling af oplysninger i relation til indleverede medier foretog tilsynet i 2018 to inspektionsbesøg i centret, hvor centrets beholdning blev kontrolleret ved stikprøver, gennemgang af centrets dokumentation samt drøftelser med udvalgte medarbejdere.

! **Tilsynets bemærkninger**

Tilsynets kontrol af CFCS' behandling af oplysninger i relation til indleverede medier viste, at centret på tidspunktet for tilsynets første inspektionsbesøg ikke iagttog lovgivningens krav til sikkerhedsforanstaltninger i CFCS-lovens § 18, stk. 1. Kontrollen viste tillige, at centrets interne retningslinjer indeholdt procedurer, som ikke var i overensstemmelse med CFCS-lovens bestemmelser.

Tilsynet noterer sig imidlertid, at CFCS på tidspunktet for tilsynets andet inspektionsbesøg havde iværksat en række tiltag med henblik på at sikre, at behandlingen af oplysninger i relation til indleverede medier finder sted i overensstemmelse med CFCS-lovens § 18, stk. 1, herunder at centret havde revideret sine interne retningslinjer for behandling af indleverede medier.

1.2.3 Kontrol af CFCS' videregivelse af oplysninger

Tilsynet har i 2018 løbende foretaget kontrol af CFCS' videregivelse af data indeholdende personoplysninger til andre myndigheder, virksomheder og udenlandske samarbejdspartnere med fokus på centrets overholdelse af CFCS-lovens §§ 10 og 16 og CFCS-retningslinjerne.

! **Tilsynets bemærkninger**
Tilsynets kontrol af CFCS' videregivelse af data indeholdende personoplysninger til andre myndigheder, virksomheder og samarbejdspartnere viste, at videregivelserne i alle tilfælde er sket under iagttagelse af lovgivningens bestemmelser herom.

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

Tilsynet har i 2018 foretaget kontrol af CFCS' udveksling af data indeholdende personoplysninger, der stammer fra indgreb i meddelelseshemmeligheden, med den øvrige del af FE med fokus på centrets overholdelse af bestemmelserne i CFCS-retningslinjerne.

Tilsynet modtager løbende orienteringer fra CFCS om centrets udveksling af data, der stammer fra indgreb i meddelelseshemmeligheden, med den øvrige del af FE. Vedrørende 2018 har tilsynet modtaget i alt 24 orienteringer i form af udfyldte udvekslingsformularer, som ikke gav tilsynet anledning til spørgsmål til CFCS.

Som supplement til kontrollen af udvekslingsformularerne udtrak tilsynet løbende stikprøver i CFCS' hændelseshåndteringssystem for at vurdere, om de udvekslede data var relevante for den konkrete sag.

! **Tilsynets bemærkninger**
Tilsynets kontrol af CFCS' udveksling af data indeholdende personoplysninger, der stammer fra indgreb i meddelelseshemmeligheden, med den øvrige del af FE viste, at udvekslingerne er sket under iagttagelse af CFCS-retningslinjernes bestemmelser herom, men at der i ét tilfælde ikke forelå forudgående juridisk godkendelse heraf som foreskrevet i centrets interne retningslinjer.

På baggrund af kontrollen opfordrede tilsynet CFCS til at sikre en ensrettet dokumentation og registrering af centrets udvekslinger, herunder med henblik på at kunne foretage en effektiv kontrol heraf.

> Tilsynets kontrol af CFCS' behandling af oplysninger i relation til indleverede medier viste, at centret på tidspunktet for tilsynets første inspektionsbesøg ikke iagttog lovgivningens krav til sikkerhedsforanstaltninger i CFCS-lovens § 18, stk. 1. Kontrollen viste tillige, at centrets interne retningslinjer indeholdt procedurer, som ikke var i overensstemmelse med CFCS-lovens bestemmelser.

1.2.5 Kontrol af arbejdsstationer i CFCS

Tilsynet har i 2018 foretaget kontrol af et antal medarbejderes arbejdsstationer med fokus på medarbejdernes behandling af oplysninger om fysiske personer, herunder de pågældendes kendskab til reglerne herom.

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

! **Tilsynets bemærkninger**

Tilsynets kontrol af udvalgte arbejdsstationer viste, at samtlige medarbejdere behandlede oplysninger om fysiske personer i overensstemmelse med CFCS-loven, og at medarbejderne generelt var opmærksomme på, at behandling af sådanne oplysninger sker i overensstemmelse med loven og centrets interne retningslinjer.

1.2.6 Kontrol af CFCS' interne kontrol

Tilsynet har ved sin kontrol af CFCS i 2018 foretaget kontrol af centrets interne kontrol. Kontrollen har omfattet CFCS' interne kontrol i 2018 samt centrets planlægning heraf for 2019. Kontrollen er foretaget ved gennemgang af udleveret dokumentation og drøftelser med centret.

Tilsynet foretog i 2016 og 2017 tilsvarende kontroller af CFCS' interne kontrol. Kontrollerne viste, at centrets interne kontrol ikke har været tilrettelagt på baggrund af en dokumenteret risiko- og væsentlighedsvurdering. På denne baggrund tilkendegav tilsynet i 2016 og 2017 overfor CFCS, at centret bør tilrettelægge sin interne kontrol på baggrund af en årlig risiko- og væsentlighedsvurdering.

Tilsynet havde på tidspunktet for afslutningen af kontrollen ikke modtaget afrapportering vedrørende de afviklede kontroller, ligesom tilsynet ikke havde modtaget en dokumenteret og ledelsesgodkendt risiko- og væsentlighedsvurdering. CFCS har imidlertid i 2019 redegjort for status på centrets interne kontrol i 2018.

! **Tilsynets bemærkninger**

Tilsynet finder det kritisabelt, at CFCS – som adviseret i 2016 og 2017 – ikke har tilrettelagt centrets interne kontrol på baggrund af en dokumenteret og ledelsesgodkendt risiko- og væsentlighedsvurdering.

Sammenholdt med manglende afrapportering vedrørende CFCS' afviklede kontroller i 2018 har tilsynet på det grundlag, som forelå på tidspunktet for afslutningen af kontrollen, ikke kunnet vurdere, hvorvidt centrets interne kontrol i 2018 har været tilfredsstillende.

Tilsynet noterer sig imidlertid, at CFCS efterfølgende har fremsendt en dokumenteret og ledelsesgodkendt risiko- og væsentlighedsvurdering samt afrapportering på afviklede interne kontroller i 2018.

2

Eksempler på CFCS' håndtering af cyberangreb

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

CFCS har bidraget med følgende beskrivelse af cyberangreb i 2018:

Center for Cybersikkerheds (CFCS) netsikkerhedstjeneste har til opgave at opdage, analysere og bidrage til at imødegå it-sikkerhedshændelser hos de offentlige myndigheder og private virksomheder, der er tilsluttet sensornetværket. Denne indsats er primært fokuseret på de mest avancerede angreb, der typisk udføres af statsstøttede aktører.

Netsikkerhedstjenestens arbejde sker i tæt samarbejde med CFCS' Cybersituationscenter, der foruden de tilsluttede organisationer også har et særligt fokus på at analysere og informere om aktuelle cyberangreb, der påvirker dansk kritisk infrastruktur, herunder de seks samfundskritiske sektorer i Danmark.

I 2018 har Netsikkerhedstjenesten og Cybersituationscentret håndteret en række it-sikkerhedshændelser, hvoraf størstedelen af angrebene var været domineret af forskellige former for social engineering, herunder angreb via e-mail i form af phishing, og som fortsat anses som en alvorlig trussel mod centrets tilsluttede organisationer.

Foruden social engineering observeres der generelt mange rekognosceringsforsøg mod centrets tilsluttede organisationer, hvor angriberen forsøger at opnå viden om potentielle ofres it-systemer, som kan udnyttes i senere angreb. Dette sker eksempelvis ved at angriberne udfører scanninger af organisationernes internetvendte tjenester.

Af andre typer sager blev der i flere tilfælde konstateret, at angribere med succes havde udnyttet sårbarheder i organisationers software til at inficere systemerne med malware. Heriblandt var der konkrete eksempler på inficeringer med såkaldte coin-minere, der udnytter den inficerede maskines regnekraft til at generere virtuel valuta på vegne af angriberen.

Derudover blev der i flere tilfælde observeret et antal brute force-relaterede angrebsforsøg mod forskellige tilsluttede organisationer. Angriberne forsøgte at tiltvinge sig adgang til organisationers it-systemer via en række automatiserede login-forespørgsler mod specifikke softwaretjenester hos dem. I disse konkrete tilfælde opnåede angriberne dog ikke adgang til systemerne.

3 Statistik vedrørende CFCS' behandling af oplysninger

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

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

CFCS har bidraget med følgende data for 2018:

Tabel 1 Modtagne klagesager over CFCS' behandling af personoplysninger

Kategorier	2018
Klagesager modtaget i CFCS	0
Klagesager modtaget i tilsynet	0

Tabel 2 Aktindsigtssager

Kategorier	2018
Fuld aktindsigt	1
Delvis aktindsigt	0
Afslag på aktindsigt	7
Ingen dokumenter lokaliseret til at give eller afslå aktindsigt i	2
Total	**10**

Tabel 3 Sikkerhedshændelser* efter alvorlighedsgrad

Kategorier	2018
Alvorlige cyberangreb	0
Større cyberangreb	1
Moderate cyberangreb	12
Mindre cyberangreb	159
None**	740
Total	**912**

* Sikkerhedshændelser defineres i overensstemmelse med § 2, nr. 1, i lov om Center for Cybersikkerhed.
** Kategorien er omdøbt fra "Falske positive" til "None", da en falsk positiv hændelse ikke har haft en indvirkning på kunden og derved ikke var en retvisende beskrivelse for denne kategori. Ved at kalde kategorien "None" får man en mere retvisende kategori, da det herved inkluderer alle de sikkerhedshændelser, som ikke har haft en indvirkning på kunden.

CFCS har herudover oplyst følgende om antallet af videregivelser af oplysninger, herunder personoplysninger der stammer fra indgreb i meddelelseshemmeligheden, til andre myndigheder, virksomheder og samarbejdspartnere samt antallet af udvekslinger af tilsvarende oplysninger med den øvrige del af FE:

Tabel 4 CFCS' videregivelser og udvekslinger af oplysninger*

Kategorier	2018
Videregivelser	109
Udvekslinger	24

* Antallet af CFCS' netsikkerhedstjenestes videregivelser af oplysninger, herunder oplysninger der stammer fra indgreb i meddelelseshemmeligheden, omfatter samtlige videregivne oplysninger, herunder om fysiske og juridiske personer, samt oplysninger, der ikke er personhenførbare. Se desuden tilsynets kontrol heraf, jf. afsnit 1.2.3.

4 Presseomtale i 2018

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

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

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

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.

Den 1. juli 2014 trådte lov nr. 713 af 26. juni 2014 om Center for Cybersikkerhed (CFCS) i kraft (herefter CFCS-loven). Med loven er CFCS' muligheder for at beskytte Danmark mod cyberangreb styrket. Styrkelsen er blandt andet sket ved at udvide centrets muligheder for at undersøge sikkerhedshændelser, herunder cyberangreb, i samarbejde med myndigheder og virksomheder, således at der i større omfang end hidtil kan indhentes de informationer, som er nødvendige for at afklare, hvilke angrebsværktøjer og -metoder som er anvendt ved sikkerhedshændelser. Loven indebærer tillige, at en række af de centrale databeskyttelsesprincipper ligeledes finder anvendelse på CFCS' virksomhed.

Med loven er det yderligere bestemt, at Tilsynet med Efterretningstjenesterne, der som et uafhængigt kontrolorgan fører tilsyn med, at PET behandler personoplysninger overensstemmelse med PET-lovgivningen, og at FE behandler oplysninger om i Danmark hjemmehørende fysiske og juridiske personer i overensstemmelse med FE-lovgivningen, tillige skal føre tilsyn med, at CFCS' behandling af oplysninger om fysiske personer er i overensstemmelse med CFCS-lovgivningen.

> 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.

2. Tilsynet med Efterretningstjenesterne

Tilsynet er et særligt uafhængigt kontrolorgan, der fører tilsyn med, at PET, FE og CFCS behandler personoplysninger i overensstemmelse med lovgivningen.

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

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

Medlemmerne er:

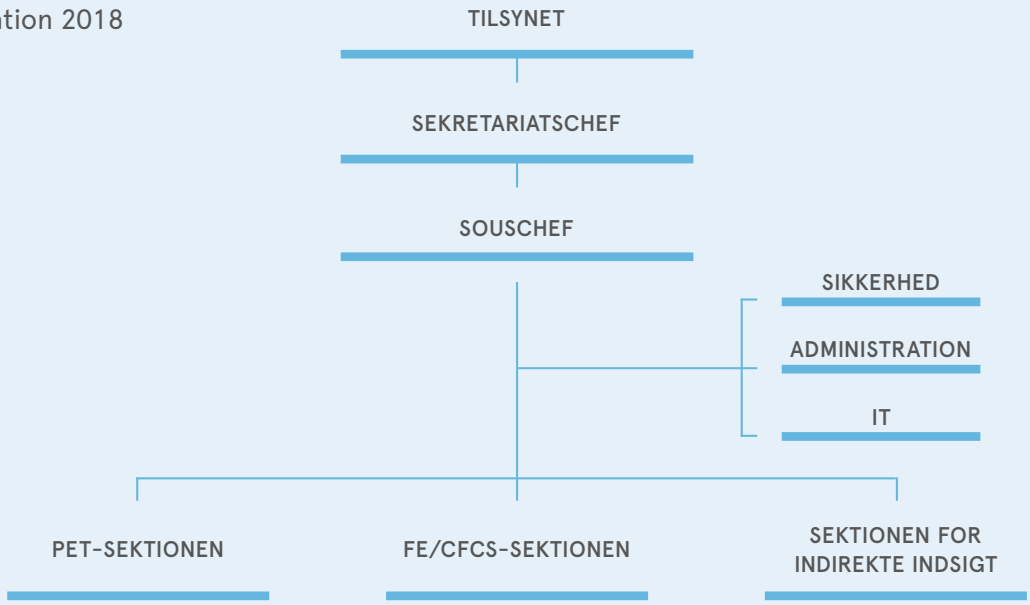
- landsdommer Michael Kistrup, Østre Landsret (formand)
- professor Jørgen Grønnegård Christensen, Aarhus Universitet
- bestyrelsesformand Erik Jacobsen, Roskilde Universitet
- juridisk chef Pernille Christensen, Kommunernes Landsforening
- professor Henrik Udsen, Københavns Universitet

Medlemmerne udpeges for en periode på fire år med mulighed for genbeskikkelse for yderligere fire år. Ved tilsynets etablering i 2014 blev to medlemmer udpeget for to år med mulighed for genbeskikkelse for yderligere fire år med henblik på at sikre mod en samtidig og fuldstændig udskiftning af tilsynets medlemmer, idet de efterfølgende funktionsperioder er forskudt to år i forhold til hinanden.

Tilsynet bistås af et sekretariat, der alene er undergivet tilsynets instruktion. Tilsynet bestemmer selv, hvem der skal ansættes til sekretariatet, herunder hvilken uddannelsesmæssig baggrund og øvrige kvalifikationer de pågældende skal have. Ved udgangen af 2018 bestod sekretariatet af en sekretariatschef, der varetager den daglige ledelse af sekretariatet, en souschef, tre jurister, en it-konsulent og en kontorfunktionær.

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

Organisation 2018



2.1 Tilsynets opgaver i forhold til CFCS

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

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

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

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

2.2 Tilsynets adgang til oplysninger i CFCS

Tilsynet kan hos CFCS kræve enhver oplysning og alt materiale, der er af betydning for tilsynets virksomhed, og tilsynet har til enhver tid adgang til alle lokaler, hvorfra der er adgang til de oplysninger, som behandles, eller hvor tekniske hjælpemidler anvendes. Tilsynet kan endvidere afkræve CFCS skriftlige udtalelser om faktiske og retlige forhold af betydning for tilsynets

kontrolvirksomhed, ligesom tilsynet kan anmode om, at en repræsentant for centret er til stede med henblik på at redegøre for de behandlede sager.

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

2.3 Tilsynets reaktionsmuligheder

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

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

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

Tilsynet afgav senest en årlig redegørelse om sin virksomhed til forsvarsministeren i maj 2018. Redegørelsen blev offentliggjort i juni 2018.

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

3. Retsgrundlag

1) Lov om Center for Cybersikkerhed (CFCS) (lovbekendtgørelse nr. 713 af 25. juni 2014, som senest ændret ved lov nr. 443 af 8. maj 2018) (CFCS-loven).

2) Forsvarsministeriets retningslinjer vedrørende behandling af data i og fra Center for Cybersikkerheds netsikkerhedstjeneste (CFCS-retningslinjerne), udstedt den 30. juni 2014.

3.1 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 myndigheder på Forsvarsministeriets område samt hos øvrige 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.

CFCS' netsikkerhedstjeneste er betegnelsen for CFCS' 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 vil der som hidtil blive 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.

En myndighed eller virksomhed, der tilsluttes netsikkerhedstjenesten, vil modtage en sikkerhedsydelse, der er tilpasset den enkelte myndigheds eller virksomheds behov. Der vil eksempelvis kunne ske en monitorering af myndighedens eller virksomhedens forbindelse til internettet, således at netsikkerhedstjenesten ved hjælp af f.eks. en lokalt placeret alarmenhed kan opdage og analysere sikkerhedshændelser. På den baggrund – og på baggrund af tilsvarende analyser hos de øvrige tilsluttede myndigheder og virksomheder – kan netsikkerhedstjenesten dels alarmere myndigheden eller virksomheden, når der konstateres konkrete sikkerhedshændelser, dels udsende mere generelle varslinger. Desuden vil tilsluttede myndigheder og virksomheder

kunne modtage varslinger på baggrund af oplysninger, som CFCS modtager fra FEs udenrigsefterretningstjeneste, andre netsikkerhedstjenester og andre udenlandske samarbejdspartnere. Netsikkerhedstjenesten vil desuden yde rådgivning om informationssikkerhed til de tilsluttede myndigheder og kunne yde bistand, hvis en myndighed eller virksomhed rammes af en alvorlig sikkerhedshændelse.

3.2 Om indgreb i meddelelseshemmeligheden, jf. CFCS-lovens §§ 4-7

Bestemmelserne i lovens §§ 4 og 5, der indholdsmæssigt er identiske, indebærer, at CFCS' netsikkerhedstjeneste uden retskendelse kan behandle pakke- og trafikdata hidrørende fra netværk hos tilsluttede myndigheder og virksomheder og hos myndigheder på Forsvarsministeriets område 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.

Reguleringen af netsikkerhedstjenestens adgang til at foretage indgreb i meddelelseshemmeligheden på henholdsvis det civile og det militære område er opdelt i to bestemmelser, da der på enkelte områder gælder særlige regler for det militære område for hermed at sikre, at der ikke foretages en indskrænkning i forhold til de muligheder for monitorering, som MILCERT tidligere har haft. På Forsvarsministeriets område, hvor der i betydeligt omfang håndteres klassificerede oplysninger, vil der således fortsat være behov for en videre adgang til at analysere monitorerede data og til at videregive data til relevante samarbejdspartnere.

Det følger af lovens § 6, at en myndighed eller virksomhed, som ikke er tilsluttet CFCS' netsikkerhedstjeneste, ved begrundet mistanke om en sikkerhedshændelse midlertidigt kan tilsluttes netsikkerhedstjenesten, som herefter uden retskendelse kan behandle pakke- og trafikdata hidrørende fra netværk hos myndigheden eller virksomheden, når

1) myndigheden eller virksomheden har anmodet CFCS om at blive midlertidigt tilsluttet og givet skriftligt samtykke til behandlingen,
2) behandlingen vurderes at kunne bidrage væsentligt til CFCS muligheder for at sikre informations- og kommunikationsteknologisk infrastruktur, som samfundsvigtige funktioner er afhængige af, og
3) den midlertidige tilslutning har en varighed på højst to måneder.

En midlertidig tilslutning kan ske i forhold til myndigheder og virksomheder, som ikke normalt er udsat for et sådant trusselsbillede, at en fast tilslutning til netsikkerhedstjenesten er hensigtsmæssig, men som på grund af aktuelle begivenheder i en kortere periode er udsat for et så konkret trusselsbillede, at der er behov for den ekstra sikkerhed, som en tilslutning indebærer. En midlertidig tilslutning kan også ske, hvis virksomheder, der ikke er beskæftiget med samfundsvigtige funktioner, rammes af særligt alvorlige cyberangreb.

Ved begrundet mistanke om en sikkerhedshændelse kan netsikkerhedstjenesten efter lovens § 7 uden retskendelse behandle data, som er indeholdt i eller hidrører fra et informationssystem, der anvendes af en myndighed eller virksomhed, når

1) myndigheden eller virksomheden har anmodet CFCS om bistand, stillet informationssystemet

eller dataene herfra til rådighed for netsikkerhedstjenesten og givet skriftligt samtykke til, at netsikkerhedstjenesten behandler dataene, og
2) behandlingen vurderes at kunne bidrage væsentligt til CFCS' muligheder for at sikre informations- og kommunikationsteknologisk infrastruktur, som samfundsvigtige funktioner er afhængige af.

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

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

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

1) den pågældende person har givet sit udtrykkelige samtykke hertil,
2) behandlingen er nødvendig af hensyn til opfyldelsen af en aftale, som den pågældende person er part i, eller af hensyn til gennemførelse af foranstaltninger, der træffes på den pågældende persons anmodning forud for indgåelsen af en sådan aftale,
3) behandlingen er nødvendig af hensyn til udførelsen af en opgave i samfundets interesse,
4) behandlingen er nødvendig til beskyttelse af væsentlige hensyn til statens sikkerhed eller rigets forsvar,
5) behandlingen er nødvendig af hensyn til udførelsen af en opgave, der henhører under offentlig myndighedsudøvelse, som CFCS eller en tredjemand, til hvem oplysningerne videregives, har fået pålagt,
6) behandlingen er nødvendig for, at CFCS eller den tredjemand, til hvem oplysningerne videregives, kan forfølge en berettiget interesse, og hensynet til den pågældende person ikke overstiger denne interesse eller
7) behandlingen vedrører personoplysninger, der er omfattet af kapitel 4 (indgreb i meddelelseshemmeligheden).

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

Der må ikke behandles personoplysninger om racemæssig eller etnisk baggrund, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssige tilhørsforhold og personoplysninger om

helbredsmæssige og seksuelle forhold, jf. lovens § 11, stk. 1. Efter bestemmelsens stk. 2 gælder dette dog ikke, hvis

1) den pågældende person har givet sit udtrykkelige samtykke til en sådan behandling,
2) behandlingen vedrører personoplysninger, som er blevet offentliggjort af den pågældende person,
3) behandlingen er nødvendig for, at et retskrav kan fastlægges, gøres gældende eller forsvares,
4) behandlingen er nødvendig til beskyttelse af væsentlige hensyn til statens sikkerhed eller rigets forsvar eller
5) behandlingen vedrører personoplysninger, der er omfattet af kapitel 4 (indgreb i meddelelseshemmeligheden).

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

1) den pågældende person har givet sit udtrykkelige samtykke til videregivelsen,
2) videregivelsen sker til varetagelse af private eller offentlige interesser, der klart overstiger hensynet til de interesser, der begrunder hemmeligholdelse, herunder hensynet til den, oplysningen angår,
3) videregivelsen er nødvendig for udførelsen af en myndigheds virksomhed eller påkrævet for en afgørelse, som myndigheden skal træffe,
4) videregivelsen er nødvendig for udførelsen af en persons eller virksomheds opgaver for det offentlige eller
5) videregivelsen omfatter personoplysninger, der er omfattet af kapitel 4 (indgreb i meddelelseshemmeligheden).

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

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

3.4 Om analyse, videregivelse og sletning af data, jf. CFCS-lovens §§ 15-17 og CFCS-retningslinjernes § 2 og §§ 4-6

Det følger af lovens § 15, at analyse af pakkedata, der er omfattet af lovens §§ 4, 6 og 7 (indgreb i meddelelseshemmeligheden), kun må finde sted ved begrundet mistanke om en sikkerhedshændelse og kun i det omfang, det er nødvendigt for afklaring af forhold vedrørende hændelsen. Bestemmelsen fastsætter rammerne for CFCS' netsikkerhedstjenestes adgang til at analysere pakkedata, der er omfattet af de nævnte bestemmelser. Som led i netsikkerhedstjenestens drift sker der løbende en fuldautomatisk behandling af data fra de tilsluttede myndigheder og virk-

somheders netværkskommunikation med henblik på at identificere mulige sikkerhedshændelser. Bestemmelsen indebærer, at netsikkerhedstjenestens sikkerhedsanalytikere kun må foretage en analyse af pakkedata, hvis der er en begrundet mistanke om en sikkerhedshændelse, og da kun i det omfang det er nødvendigt for afklaring af forhold vedrørende hændelsen.

Netsikkerhedstjenestens aktiviteter på det militære område, jf. lovens § 5, er ikke omfattet af lovens § 15, men reguleres nærmere af administrative retningslinjer. Ifølge § 4, stk. 1, i CFCS-retningslinjerne må analyse af pakkedata hidrørende fra netværk hos myndigheder på Forsvarsministeriets område, jf. lovens § 5, kun finde sted i følgende tilfælde:

1) Ved begrundet mistanke om en sikkerhedshændelse.
2) Som led i det løbende arbejde med at understøtte et højt informationssikkerhedsniveau på Forsvarsministeriets område, herunder ved kontrol af, om kommunikation indeholder klassificeret materiale.

Efter bestemmelsens stk. 2 må analyse efter stk. 1 kun ske i det omfang, det er nødvendigt for afklaring af forhold vedrørende hændelsen eller nødvendigt for at understøtte et højt informationssikkerhedsniveau på Forsvarsministeriets område.

Ifølge lovens § 16 kan data, der er omfattet af lovens §§ 4, 6 og 7 (indgreb i meddelelseshemmeligheden), kun videregives i følgende tilfælde:

1) Ved begrundet mistanke om en sikkerhedshændelse kan data videregives til politiet.
2) Ved begrundet mistanke om en sikkerhedshændelse, og hvis det er nødvendigt for udførelsen af netsikkerhedstjenestens opgaver, kan trafikdata videregives til danske myndigheder, udbydere af offentlige elektroniske kommunikationsnet og -tjenester, andre netsikkerhedstjenester og virksomheder, der er omfattet af §§ 4, 6 og 7, samt til myndigheder og virksomheder i øvrigt i forbindelse med CFCS' udsendelse af sikkerhedsvarslinger.

Bestemmelsen regulerer CFCS' muligheder for at videregive data, der er omfattet af lovens §§ 4, 6 og 7 og dermed behandles på baggrund af indgreb i meddelelseshemmeligheden. Med lovens § 16, nr. 1, sikres, at centret kan videregive alle relevante oplysninger til politiet i de tilfælde, hvor det kan være relevant for politiet at indlede en strafferetlig efterforskning. Kravet om, at der skal være tale om en begrundet mistanke om en sikkerhedshændelse, indebærer, at CFCS alene kan videregive de pågældende data, hvis der foreligger konkrete indikationer, der peger i retning af, at en sikkerhedshændelse har fundet eller vil finde sted.

Lovens § 16, nr. 2, om muligheden for at videregive trafikdata til blandt andre udbydere af offentlige elektroniske kommunikationsnet og -tjenester indebærer, at især teleselskaber kan forbedre deres sikkerhedssystemer, således at den informations- og kommunikationsteknologiske infrastruktur, som samfundsvigtige funktioner i overvejende grad er afhængige af, kan sikres yderligere, f.eks. ved at teleselskaberne informeres om IP-adresser, der anvendes ved cyberangreb. En af CFCS' vigtigste forebyggende aktiviteter er udsendelse af sikkerhedsvarslinger, hvor myndigheder, virksomheder, andre netsikkerhedstjenester mv. underrettes om særligt alvorlige sikkerhedshændelser. Sikkerhedsvarslingerne giver modtagerne mulighed for at styrke deres egen forebyggelse mod angreb (f.eks. ved at blokere for trafik fra IP-adresser, der indgår i hackeres angrebsinfrastruktur) og undersøge, om de har været udsat for angreb (f.eks. ved at gennemsøge logfiler for e-mails fra afsendere, der har angrebet andre myndigheder eller virksomheder). Med bestemmelsen i nr. 2 er der derfor givet CFCS mulighed for at udsende sikkerhedsvarslinger, som indeholder trafikdata, der kan styrke modtagernes informations-

sikkerhed. Videregivelse af trafikdata efter nr. 2 forudsætter, at der er begrundet mistanke om en sikkerhedshændelse, og at det konkret vurderes, at videregivelsen er nødvendig for udførelsen af netsikkerhedstjenestens opgaver. Indeholder videregivelsen personoplysninger, vil principperne om relevans og proportionalitet, jf. lovens § 9, stk. 2, tillige skulle iagttages, således at der alene kan videregives personoplysninger, som er relevante og tilstrækkelige for at opnå formålet med den konkrete videregivelse.

Lovens § 16 skal endvidere ses i sammenhæng med lovens § 12, som generelt regulerer CFCS' adgang til at videregive personoplysninger om strafbare forhold, væsentlige sociale problemer og andre rent private forhold end de, der er nævnt i lovens § 11, stk. 1. Erfaringsmæssigt har CFCS kun i meget sjældne tilfælde behov for at videregive personoplysninger af de nævnte typer, men i forbindelse med alvorlige cyberangreb kan der være behov for at videregive personoplysninger om strafbare forhold til politiet. Lovens § 12, stk. 2, nr. 5, giver hjemmel til videregivelse af de nævnte typer af personoplysninger, hvis oplysningerne er omfattet af kapitel 4 (indgreb i meddelelseshemmeligheden). Spørgsmålet om videregivelse skal derefter vurderes efter lovens § 16.

Netsikkerhedstjenestens aktiviteter på det militære område, jf. lovens § 5, er ikke omfattet af lovens § 16, men reguleres nærmere af administrative retningslinjer. Ifølge § 6 i CFCS-retningslinjerne må data, der er omfattet af lovens § 5, kun videregives af CFCS, når

1) videregivelsen er nødvendig for at understøtte et højt informationssikkerhedsniveau, og
2) videregivelsen sker med udtrykkeligt angivne og saglige formål, idet enhver videregivelse af data skal registreres af CFCS.

I lovforslagets almindelige bemærkninger 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 i CFCS-retningslinjerne fastsat, at CFCS kun må udveksle data, der er omfattet af lovens §§ 4, 6 og 7, 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,

idet enhver udveksling af data skal registreres af CFCS.

Tilsvarende følger det af § 5 i CFCS-retningslinjerne, at CFCS kun må udveksle data, der er omfattet af lovens § 5, med den øvrige del af FE, når

1) udvekslingen er nødvendig for at understøtte et højt informationssikkerhedsniveau, og
2) udvekslingen sker med udtrykkeligt angivne og saglige formål,

idet enhver udveksling af data skal registreres af CFCS.

Ifølge lovens § 17, stk. 1, skal data, der er omfattet af kapitel 4 (indgreb i meddelelseshemmeligheden), 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 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 denne bestemmelse ske en løbende vurdering af de behandlede data med henblik på at sikre, at data, der ikke længere er relevante i forhold til netsikkerhedstjenestens formål og aktiviteter, straks slettes.

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

1) data, der knytter sig til en sikkerhedshændelse, højst opbevares i 3 år og
2) 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 treårige periode igen konstateres anvendt i forbindelse med en sikkerhedshændelse, vil en ny treårig periode begynde. Fristerne i stk. 2, regnes fra tidspunktet for CFCS' registrering af de pågældende data, jf. stk. 3.

Lovens § 17, stk. 1 og 2, finder ikke anvendelse på data, der er videregivet i medfør af lovens § 16, jf. lovens § 17, stk. 4.

3.5 Om sikkerhedsforanstaltninger i forbindelse med centrets 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.

Årsredegørelse 2018
Center for Cybersikkerhed
Udgivet af Tilsynet med Efterretningstjenesterne, juni 2019

Layout + illustrationer: Eckardt ApS
Portrætfotos: Lars Engelgaar

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

Medlemmer af Tilsynet med Efterretningstjenesterne

Landsdommer Michael Kistrup, Østre Landsret (formand)
Juridisk chef Pernille Christensen, Kommunernes Landsforening
Professor Henrik Udsen, Københavns Universitet
Professor Jørgen Grønnegård Christensen, Aarhus Universitet
Bestyrelsesformand Erik Jacobsen, Roskilde Universitet

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