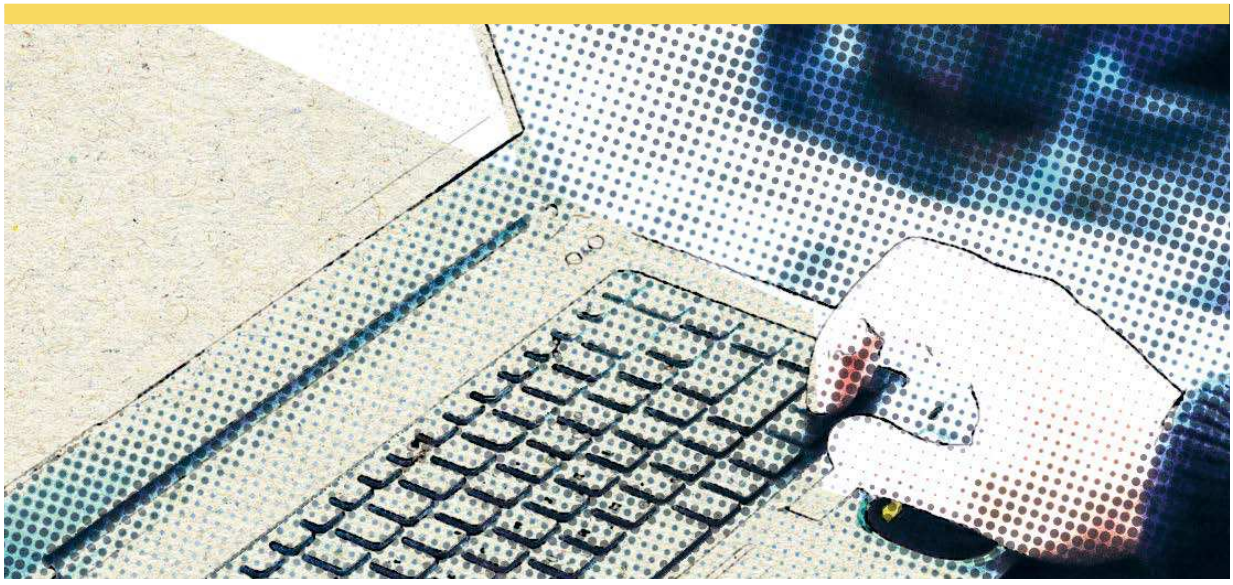


Årsredegørelse 2016

Center for Cybersikkerhed

Indhold

Til forsvarsministeren

I overensstemmelse med § 24 i lov om Center for Cybersikkerhed (lov nr. 713 af 25. juni 2014) afgiver Tilsynet med Efterretningstjenesterne hermed redegørelse om sin virksomhed vedrørende Center for Cybersikkerhed for 2016. Redegørelsen skal offentliggøres.

København, maj 2017

Ulla Staal

Formand for Tilsynet med Efterretningstjenesterne


BERLIN

Forord

Lov om Center for Cybersikkerhed trådte i kraft den 1. juli 2014, og ifølge loven skal **Tilsynet med Efterretningstjenesterne** som et særligt uafhængigt kontrolorgan føre 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.

Tilsynet har i 2016 gennemført omfattende og intensive kontroller med CFCS' behandling af oplysninger om fysiske personer, hvilket blandt andet har været muliggjort af yderligere ansættelser til sekretariatet af personer med relevante kompetenceprofiler og af en fortsat øget indsigt i revisionsmetodik, risikovurdering og testmodeller med deraf følgende optimering af tilsynets kontroller. Med udgangen af året må tilsynet inden for de aktuelt givne rammer anses for fuldt udbygget.

Sigtet med redegørelsen er at give information om karakteren af det tilsyn, der udøves vedrørende CFCS, herunder en generel beskrivelse af hvilke forhold tilsynet i 2016 har valgt særligt at interessere sig for. Redegørelsen indeholder endvidere nærmere angivne statistiske oplysninger om CFCS' behandling af personoplysninger samt oplysninger om, i hvor mange tilfælde tilsynet har fundet, at CFCS' behandling af personoplysninger ikke har været i overensstemmelse med reglerne. Redegørelsen indeholder herudover en anonymiseret beskrivelse af to konkrete cyberangreb og en statistik over antallet af tilfælde, hvor en analytiker fra centret på baggrund af indgreb i meddelelseshemmeligheden har foretaget en analyse af data.

Ulla Staal
formand

1 Om Center for Cybersikkerhed

Center for Cybersikkerhed (CFCS) blev oprettet i 2012 som en del af Forsvarets Efterretningstjeneste (FE) til varetagelse af blandt andet følgende opgaver:

- GovCERT (Governmental Computer Emergency Response Team), der er den statslige varslingstjeneste for internettrusler
- MILCERT (Military Computer Emergency Response Team), der er varslingstjeneste for internettrusler på Forsvarsministeriets område
- National it-sikkerhedsmyndighed (bortset fra Justitsministeriets område, hvor Politiets Efterretningstjeneste (PET) varetager opgaven)
- Informationssikkerhed og beredskab på teleområdet

CFCS' hovedopgave er 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 sikkerhedshændelser på såvel det civile som det militære område.

Indtil den 1. juli 2014 var GovCERTs virksomhed reguleret af den såkaldte GovCERT-lov (lov nr. 596 af 14. juni 2011). CFCS' øvrige opgaver var ikke omfattet af denne lov, og CFCS' virksomhed blev heller ikke omfattet af lov om Forsvarets Efterretningstjeneste (FE) (herefter FE-loven), der trådte i kraft den 1. januar 2014. Bortset fra GovCERT var CFCS' virksomhed indtil den 1. juli 2014 således alene reguleret af forsvarslovens § 13 og af administrative direktiver udstedt af Forsvarsministeriet.

Den 1. juli 2014 trådte lov nr. 713 af 26. juni 2014 om Center for Cybersikkerhed (CFCS) i kraft (herefter CFCS-loven). Formålet med loven er først og fremmest at etablere et samlet lovgrundlag for CFCS, hvorved GovCERTs, MILCERTs og CFCS' øvrige aktiviteter i tilknytning til CERT-aktiviteterne under fællesbetegnelsen "netsikkerhedstjeneste" underlægges samme regulering. Med loven styrkes endvidere CFCS' muligheder for at beskytte Danmark mod cyberangreb. Styrkelsen sker blandt andet 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. Dette vil styrke mu-

ligheden for at forebygge nye og tilsvarende hændelser. Loven indebærer tillige, at en række af de centrale principper i persondataloven også finder anvendelse på CFCS' virksomhed. Med loven er det yderligere bestemt, at Tilsynet med Efterretningstjenesterne (herefter tilsynet), der som et uafhængigt kontrolorgan fører tilsyn med, at PET behandler oplysninger om fysiske og juridiske personer i 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.

I medfør af CFCS-loven har Forsvarsministeriet med ikrafttræden den 1. juli 2014 udstedt Retningslinjer vedrørende behandling af data i og fra Center for Cybersikkerheds netsikkerhedstjeneste (herefter CFCS-retningslinjerne).

Ved lov nr. 1567 af 15. december 2015 om net- og informationssikkerhed (herefter NIS-loven), der trådte i kraft den 1. juli 2016, er reguleringen af informationssikkerhed og beredskab på teleområdet samlet i en ny lov, og samtidig er der sket en skærpelse af kravene til teleudbydernes informationssikkerhed med henblik på at styrke net- og informationssikkerheden i Danmark. CFCS fører tilsyn med overholdelsen af loven og regler udstedt i medfør heraf.

> CFCS' hovedopgave er at understøtte et højt informationssikkerhedsniveau i den informations- og kommunikationsteknologiske infrastruktur, som samfundsvigtige funktioner er afhængige af.

2 Tilsynet med Efterretningstjenesterne

Tilsynet er oprettet ved lov om Politiets Efterretningstjeneste (PET) (herefter PET-loven), der ligesom FE-loven trådte i kraft den 1. januar 2014. Tilsynet er et særligt uafhængigt kontrolorgan, der fører tilsyn med, at PET behandler oplysninger om fysiske og juridiske personer i overensstemmelse med PET-lovgivningen, og at FE behandler oplysninger om i Danmark hjemmehørende fysiske og juridiske personer i overensstemmelse med FE-lovgivningen. Efter ikrafttrædelsen den 1. juli 2014 af CFCS-loven har tilsynet tillige ført kontrol med, at CFCS behandler oplysninger om fysiske personer i overensstemmelse med CFCS-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 Ulla Staal, Østre Landsret (formand)
- advokat Pernille Backhausen, Sirius Advokater
- direktør Adam Wolf, Danske Regioner
- professor Jørgen Grønnegård Christensen, Aarhus Universitet
- bestyrelsesformand Erik Jacobsen, Roskilde Universitet

Med henblik på at sikre kontinuitet i tilsynets arbejde er landsdommer Ulla Staal, advokat Pernille Backhausen og direktør Adam Wolf udpeget for en periode på fire år, mens professor Jørgen Grønnegård Christensen og bestyrelsesformand Erik Jacobsen (udpeget oktober 2014) blev udpeget for en periode på to år. Samtlige medlemmer har mulighed for genbeskikkelse i yderligere fire år, og i oktober 2015 og oktober 2016 blev henholdsvis Jørgen Grønnegård Christensen og Erik Jacobsen genbeskikket for yderligere fire år.

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

Tilsynet bistås af et sekretariat, der alene er undergivet tilsynets instruktion. Tilsynet bestemmer selv, hvem der skal ansættes i sekretariatet, herunder hvilken uddannelsesmæssig baggrund og øvrige kvalifikationer, de pågældende skal have. Ved udgangen af 2016 bestod sekretariatet af en juridisk sekretariatschef, der varetager den daglige ledelse af sekretariatet, en cand.scient. pol., tre jurister, en it-konsulent og en kontorfunktionær.

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, om CFCS 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 CFCS 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 CFCS 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 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. Redegørelserne 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 sin første årlige redegørelse om sin virksomhed vedrørende CFCS til forsvarsministeren i maj 2016. Redegørelsen blev offentliggjort ultimo maj 2016.

2.4 Tilsynets arbejde og fokusområder i 2016

Tilsynet har i 2016 gennemført omfattende og intensive kontroller med CFCS' behandling af oplysninger om fysiske personer.

Tilsynets sekretariat har i gennemsnit tilbragt en halv til en hel dag om ugen hos CFCS, hvor sekretariatet har foretaget kontroller og afholdt møder med centrets personale til afklaring af spørgsmål mv. Resultatet af kontrollerne er forelagt tilsynet på månedlige møder, hvor det blandt andet er besluttet, om konkrete oplysninger mv. har givet anledning til yderligere spørgsmål til CFCS. I løbet af året har tilsynet endvidere deltaget i flere møder med CFCS, hvor typisk emner, som på forhånd var fastlagt af tilsynet, blev drøftet. Det drejede sig både om emner af konkret karakter affødt af de udførte kontroller og om emner af mere generel karakter.

Ligesom i det foregående år har tilsynet i 2016 prioriteret kontroller med fokus på CFCS' overholdelse af reglerne om indgreb i meddelelseshemmeligheden, om behandling af personoplysninger, om analyse, videregivelse og sletning af data samt om sikkerhedsforanstaltninger i forbindelse med centrets behandling af personoplysninger. Tilsynets valg af kontrolområder har været baseret på en risiko- og væsentlighedsvurdering af, hvilke områder der særligt måtte forventes at kunne give problemer, ligesom valg af metode har været tilpasset de enkelte kontrolområder. Om den nærmere gennemgang af kontrollerne på fokusområderne henvises til afsnit 3.1.

Også i 2016 har tilsynets it-konsulent bidraget væsentligt til optimering af flere af tilsynets kontroller i CFCS, herunder i relation til kontrollerne vedrørende overholdelse af reglerne om sikkerhedsforanstaltninger i forbindelse med behandling af personoplysninger. It-konsulenten har herudover navnlig bistået med vurdering af centrets it-systemer især med henblik på at sikre, at grundlaget for tilsynets stikprøvekontroller er korrekt.

Tilsynet har i 2016 fortsat sit samarbejde med revisions- og konsulentvirksomheden, som i 2015 bistod tilsynet med øget indsigt i revisionsmetodik, risikovurdering og testmodeller. Revisions- og konsulentvirksomheden har i den forbindelse udarbejdet en rapport om tilsynets kontrol og en rapport om intern kontrol samt tilsynets mulighed for efterprøvning heraf. I forhold til tilsynets kontrol konkluderede revisions- og konsulentvirksomheden generelt, at tilsynet har tilrettelagt sine procedurer hensigtsmæssigt, og at tilsynets konklusioner i forhold til de enkelte kontroller er velunderbyggede og dokumenterede. Revisions- og konsulentvirksomheden fremkom med nogle anbefalinger, som tilsynet efterfølgende har implementeret i sit arbejde.

I årets løb har tilsynet endvidere haft øget fokus på intern kontrol af egen virksomhed og har herunder implementeret nye procedurer og kontroller vedrørende informationssikkerhed.

Tilsynet har også i 2016 udbygget kontakten med udenlandske kontrolorganer, der på forskellig vis fører kontrol med deres respektive landes efterretningstjenester, for på denne måde at kunne indhente erfaringer fra internationalt regi. Tilsynet har herunder deltaget i en IIOF-konference (International Intelligence Oversight Forum), der blev afholdt i Bukarest, ligesom tilsynet i øvrigt har været i dialog om generelle emner af relevans for sin virksomhed med tilsvarende kontrolorganer i Belgien, Holland, Norge, Schweiz og Sverige.

Tilsynet afholder i oktober 2017 i samarbejde med Folketingets Udvalg vedrørende Efterretningstjenesterne en nordisk konference for tilsyn med efterretningstjenester.

Tilsynets valg af kontrolområder har været baseret på en risiko- og væsentlighedsvurdering af, hvilke områder der særligt måtte forventes at kunne give problemer, ligesom valg af metode har været tilpasset de enkelte kontrolområder.

3 Tilsynets kontrol i 2016

3.1 Egen drift-kontroller

Med henblik på at kontrollere, at CFCS i forbindelse med behandling af oplysninger om fysiske personer overholder reglerne om

- indgreb i meddelelseshemmeligheden, jf. CFCS-lovens §§ 4-7,
- behandling af personoplysninger i CFCS, jf. CFCS-lovens §§ 9-14,
- analyse, videregivelse og sletning af data, jf. CFCS-lovens §§ 15-17, og CFCS-retningslinjerne §§ 2, 4, 5 og 6, og
- sikkerhedsforanstaltninger i forbindelse med centrets behandling af personoplysninger, jf. CFCS-lovens § 18,

har tilsynet i 2016 foretaget

- stikprøvekontrol vedrørende behandling af personoplysninger i centrets elektroniske hændelseshåndteringssystem (3.1.1),
- stikprøvekontrol vedrørende behandling af personoplysninger i centrets journalsystem (3.1.2),
- kontrol vedrørende centrets samarbejde med politiet, herunder PET (3.1.3),
- kontrol vedrørende centrets udveksling af data indeholdende personoplysninger, der stammer fra indgreb i meddelelseshemmeligheden, med den øvrige del af FE (3.1.4), og
- kontrol vedrørende centrets videregivelse af data indeholdende personoplysninger, der stammer fra indgreb i meddelelseshemmeligheden, til andre myndigheder, virksomheder og samarbejdspartnere (3.1.5).

3.1.1 Stikprøvekontrol vedrørende behandling af personoplysninger i centrets elektroniske hændelseshåndteringssystem

Tilsynet har i 2016 foretaget en stikprøvekontrol vedrørende CFCS' behandling af personoplysninger i centrets elektroniske hændelseshåndteringssystem. I den forbindelse tilvejebragte og gennemgik sekretariatet et antal tilfældigt udvalgte hændelsessager og anmodede efter en konkret vurdering CFCS om uddybende bemærkninger hertil. I relation til 4 procent af de udtrukne sager havde sekretariatet spørgsmål til og/eller drøftelser med CFCS, herunder om centret havde videregivet konkrete data.

På dette grundlag blev resultatet af stikprøvekontrollen forelagt tilsynet, som besluttede, om hver enkelt oplysning var tilstrækkelig belyst, eller om der var behov for indhentelse af yderligere oplysninger eller nærmere drøftelser med centret.

! **Tilsynets bemærkninger**
Stikprøvekontrollen vedrørende CFCS' behandling af personoplysninger i centrets elektroniske hændelseshåndteringssystem viste, at CFCS har iagttaget lovgivningens bestemmelser i relation til indgreb i meddelelseshemmeligheden, til behandling af personoplysninger samt til analyse, videregivelse og sletning af data.

3.1.2 Stikprøvekontrol vedrørende behandling af personoplysninger i centrets journalsystem

Tilsynet har i 2016 foretaget en stikprøvekontrol vedrørende CFCS' behandling af personoplysninger i centrets elektroniske journal. I den forbindelse tilvejebragte og gennemgik sekretariatet et antal tilfældigt udvalgte dokumenter indeholdende personoplysninger i form af IP-adresser, e-mailadresser og domænenavne og anmodede efter en konkret vurdering CFCS om uddybende bemærkninger hertil. I relation til 16 procent af de udtrukne dokumenter havde sekretariatet spørgsmål til og/eller drøftelser med CFCS, herunder om centrets fortsatte behov for at bevare udvalgte oplysninger.

På dette grundlag blev resultatet af stikprøvekontrollen forelagt tilsynet, som besluttede, om hver enkelt oplysning var tilstrækkelig belyst, eller om der var behov for indhentelse af yderligere oplysninger eller nærmere drøftelser med centret.

! **Tilsynets bemærkninger**
Stikprøvekontrollen vedrørende CFCS' behandling af personoplysninger i centrets elektroniske journal viste, at CFCS har iagttaget lovgivningens bestemmelser herom.

Stikprøvekontrollen vedrørende CFCS' behandling af personoplysninger i centrets elektroniske hændelseshåndteringssystem viste, at CFCS har iagttaget lovgivningens bestemmelser i relation til indgreb i meddelelseshemmeligheden, til behandling af personoplysninger samt til analyse, videregivelse og sletning af data.

3.1.3 Kontrol vedrørende centrets samarbejde med politiet, herunder PET

Tilsynet har i 2016 foretaget kontrol vedrørende CFCS' samarbejde med politiet, herunder PET, i centrets elektroniske hændelseshåndteringssystem med fokus på CFCS' overholdelse af lovgivningens bestemmelser vedrørende behandling af personoplysninger og om videregivelse af data, der stammer fra indgreb i meddelelseshemmeligheden. I den forbindelse tilvejebragte og gennemgik sekretariatet hændelsessager, hvori CFCS har videregivet personoplysninger og/eller modtaget arbejdsanmodninger fra politiet, herunder PET, og anmodede efter en konkret vurdering centret om uddybende bemærkninger hertil. I relation til 5 procent af hændelsessagerne havde sekretariatet spørgsmål til og/eller drøftelser med CFCS.

På dette grundlag blev resultatet af kontrollen forelagt tilsynet, som besluttede, om hver enkelt oplysning var tilstrækkeligt belyst, eller om der var behov for indhentelse af yderligere oplysninger eller nærmere drøftelser med centret.

! **Tilsynets bemærkninger**
Kontrollen vedrørende hændelsessager, hvori CFCS har videregivet personoplysninger og/eller modtaget arbejdsanmodninger fra politiet, herunder PET, viste, at CFCS har iagttaget lovgivningens bestemmelser angående behandling og videregivelse af personoplysninger.

3.1.4 Kontrol vedrørende centrets udveksling af data indeholdende personoplysninger, der stammer fra indgreb i meddelelseshemmeligheden, med den øvrige del af FE

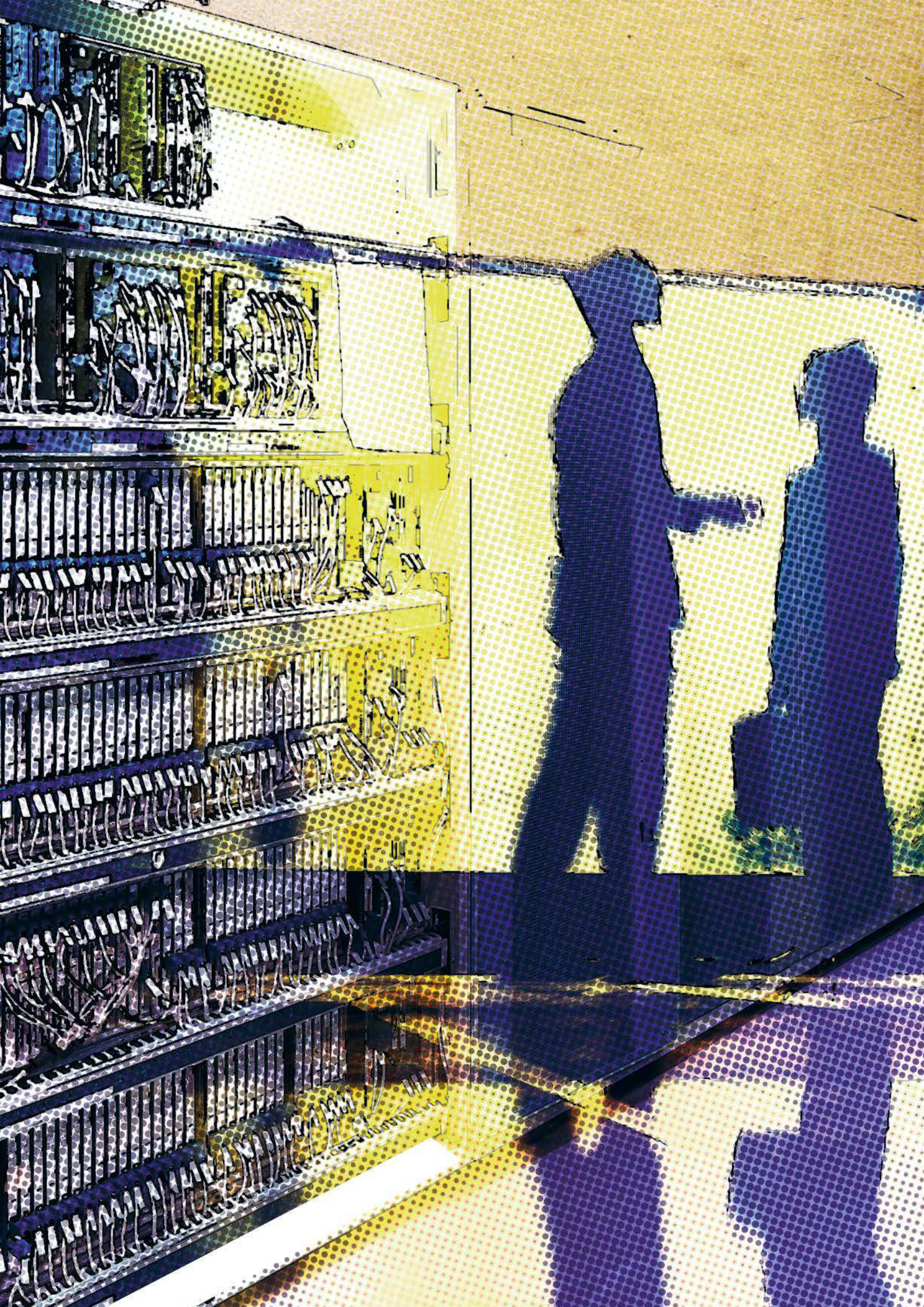
Tilsynet har i 2016 foretaget kontrol af CFCS' udveksling af data indeholdende personoplysninger, der stammer fra indgreb i meddelelseshemmeligheden, med den øvrige del af FE, med fokus på centrets overholdelse af CFCS-retningslinjernes bestemmelser herom.

Tilsynet modtager løbende orienteringer fra CFCS om centrets udveksling af data, der stammer fra indgreb i meddelelseshemmeligheden, med den øvrige del af FE. I 2016 modtog tilsynet i alt 47 orienteringer i form af udfyldte udvekslingsformularer, som ikke gav sekretariatet anledning til spørgsmål til CFCS.

Som supplement til kontrollen af udvekslingsformularerne udtrak sekretariatet en stikprøve blandt disse for at vurdere, om de udvekslede data var relevante for den konkrete sag, og sekretariatet fremsøgte i den forbindelse data vedrørende seks udvekslinger foretaget i 2016.

På dette grundlag blev resultatet af kontrollerne forelagt tilsynet, som besluttede, om de enkelte udvekslinger og data var tilstrækkelig belyst, eller om der var behov for indhentelse af yderligere oplysninger eller nærmere drøftelser med centret.

! **Tilsynets bemærkninger**
Kontrollen vedrørende 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.



3.1.5 Kontrol vedrørende centrets videregivelse af data indeholdende personoplysninger, der stammer fra indgreb i meddelelseshemmeligheden, til andre myndigheder, virksomheder og samarbejdspartnere

Tilsynet har i 2016 foretaget kontrol af CFCS' videregivelse af data indeholdende personoplysninger, der stammer fra indgreb i meddelelseshemmeligheden, til andre myndigheder, virksomheder og udenlandske samarbejdspartnere, med fokus på centrets overholdelse af CFCS-lovens § 16 og CFCS-retningslinjernes bestemmelser herom.

Tilsynet modtager kvartalsvist oversigter fra CFCS over centrets videregivelser af data, der stammer fra indgreb i meddelelseshemmeligheden, til andre myndigheder, virksomheder og samarbejdspartnere. CFCS' kvartalsvise oversigter i 2016 gav anledning til, at sekretariatet stillede nogle opklarende spørgsmål til centret, som alle blev besvaret på tilfredsstillende vis. Sekretariatet vurderede herefter, i hvilket omfang der rent faktisk var sket videregivelse af data indeholdende personoplysninger, og om videregivelserne i givet fald var sket i overensstemmelse med lovgivningens bestemmelser herom.

På dette grundlag blev resultatet af kontrollen forelagt tilsynet, som besluttede, om de enkelte videregivelser var tilstrækkelig belyst, eller om der var behov for indhentelse af yderligere oplysninger eller nærmere drøftelser med centret.

Kontrollen viste, at centret i 2016 samlet videregav data indeholdende personoplysninger, der stammer fra indgreb i meddelelseshemmeligheden, til andre myndigheder, virksomheder samt udenlandske samarbejdspartnere i 125 tilfælde fordelt på 62 sager.

! Tilsynets bemærkninger

Kontrollen vedrørende CFCS' videregivelse af data indeholdende personoplysninger, der stammer fra indgreb i meddelelseshemmeligheden, til andre myndigheder, virksomheder og samarbejdspartnere viste, at videregivelserne i alle tilfælde er sket under iagttagelse af lovgivningens bestemmelser herom.

3.1.6 Sammenfatning af tilsynets egen drift-kontroller i 2016

Tilsynets stikprøvekontrol vedrørende CFCS' behandling af personoplysninger i centrets elektroniske hændelseshåndteringssystem, jf. afsnit 3.1.1, viste i lighed med tilsvarende kontrol i 2015, at centret overholder lovgivningens bestemmelser om indgreb i meddelelseshemmeligheden, om behandling af personoplysninger samt om analyse, videregivelse og sletning af data.

Stikprøvekontrol vedrørende behandling af personoplysninger i CFCS' journalsystem viste, jf. afsnit 3.1.2, at centret overholder lovgivningens bestemmelser herom, ligesom kontrol vedrørende CFCS' samarbejde med politiet, herunder PET viste, jf. afsnit 3.1.3, at centret overholder lovgivningens bestemmelser om behandling og videregivelse af personoplysninger.

Kontrol vedrørende CFCS' udveksling af data indeholdende personoplysninger, der stammer fra indgreb i meddelelseshemmeligheden, med den øvrige del af FE, jf. afsnit 3.1.4, viste i lighed med tilsvarende kontrol i 2015, at centret overholder CFCS-retningslinjernes bestemmelser herom.

Også kontrol vedrørende CFCS' videregivelse af data indeholdende personoplysninger, der stammer fra indgreb i meddelelseshemmeligheden, til andre myndigheder, virksomheder og samarbejdspartnere, jf. afsnit 3.1.5, viste i lighed med tilsvarende kontrol i 2015, at centret overholder lovgivningens bestemmelser herom.

3.2 Opfølgning på kontroller i 2015

3.2.1 Kontrol vedrørende sikkerhedsforanstaltninger i forbindelse med centrets behandling af personoplysninger

I tilsynets redegørelse om sin virksomhed vedrørende CFCS for 2014 og 2015, afsnit 3.1.2, beskrev tilsynet en kontrol foretaget i 2015 vedrørende sikkerhedsforanstaltninger i forbindelse med centrets behandling af personoplysninger, som viste, at CFCS ikke fuldt ud levede op til lovgivningens krav om sikkerhedsforanstaltninger eller internt fastsatte retningslinjer herom i forhold til et antal observationer med tilhørende risici inden for 9 af 38 kontrollerede områder.

CFCS har efterfølgende over for tilsynet oplyst, at centret har afhjulpet hovedparten af de omhandlede risici.

Tilsynet har i 2016 foretaget en opfølgning på kontrollen heraf med henblik på at sikre, at CFCS har implementeret tilstrækkelige sikkerhedsforanstaltninger til afhjælpning af de omhandlede risici. Opfølgningen viste, at dette var tilfældet inden for 4 af de 9 kontrolområder, men at implementering af nødvendige sikkerhedsforanstaltninger i forhold til risici forbundet med et antal observationer inden for de resterende 5 kontrolområder fortsat udestår. CFCS har over for tilsynet tilkendegivet, at centret vil afhjælpe de resterende risici.

> Kontrol vedrørende CFCS' udveksling af data indeholdende personoplysninger, der stammer fra indgreb i meddelelseshemmeligheden, med den øvrige del af FE [...] viste i lighed med tilsvarende kontrol i 2015, at centret overholder CFCS-retningslinjernes bestemmelser herom.

4 CFCS' interne kontrol

Tilsynet har ved sin kontrol af CFCS i 2016 foretaget kontrol af centrets interne kontrol. Kontrollen har omfattet hele CFCS' interne kontrol i 2016 og er foretaget ved gennemgang af udleveret dokumentation, drøftelser med centret og med bistand fra en revisions- og konsulentvirksomhed.

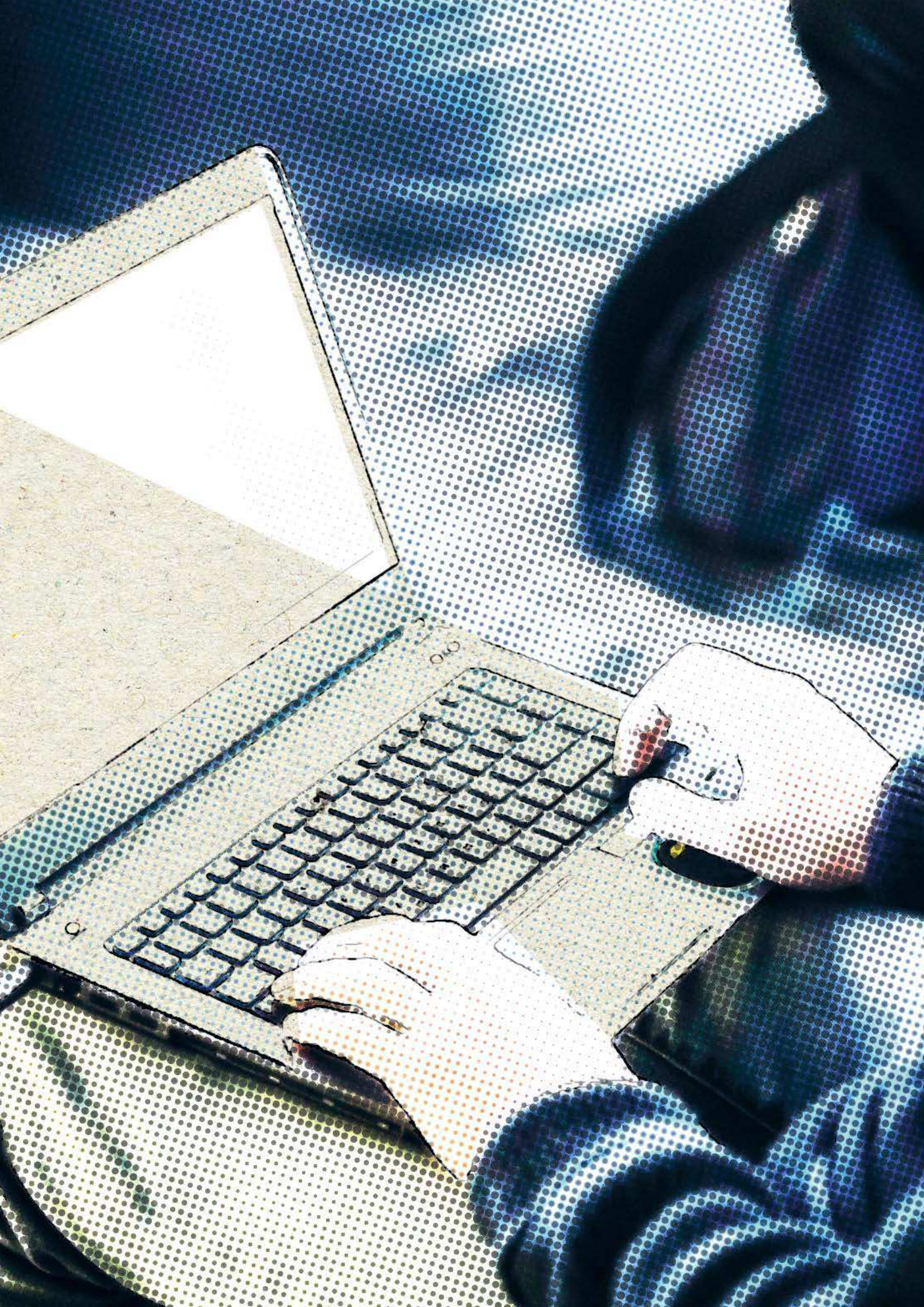
Ved vurderingen af CFCS' interne kontrol har tilsynet blandt andet henset til en rapport udarbejdet af pågældende revisions- og konsulentvirksomhed vedrørende intern kontrol og tilsynets mulighed for efterprøvning heraf, som er baseret på internationale standarder og guidelines for god revision og test af interne kontroller (ISA'erne) og på Rigsrevisionens "God offentlig revisionsskik" (GOR), jf. afsnit 2.4.

Kontrollen har vist, at CFCS har god fokus på forudgående legalitetssikring i form af undervisning af medarbejdere, tilrettelæggelse af procedurer blandt andet med forudgående juridisk godkendelse af visse handlinger mv., alt med henblik på at minimere omfanget af uberettigede handlinger.

CFCS udarbejder løbende afvigerapporter vedrørende utilsigtede hændelser med henblik på at skabe grundlag for systematisk læring. Tilsynet finder imidlertid, at CFCS i sin interne kontrol bør implementere yderligere efterfølgende legalitetskontrol, herunder stikprøvekontroller, jf. CFCS-lovens § 18, der indholdsmæssigt er identisk med persondatalovens § 41, stk. 3, og principperne i bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning (sikkerhedsbekendtgørelsen) § 5, stk. 1, 4. pkt.

CFCS bør endvidere udarbejde årlige risiko- og væsentlighedsvurderinger som grundlag for centrets valg af kontrolområder og omfang af den interne kontrol, jf. princippet i sikkerhedsbekendtgørelsens § 5, stk. 2, og i den sammenhæng bør centret løbende følge op på status på den interne kontrol og herunder vurdere, om der er behov for ændringer eller justeringer som følge af resultaterne af såvel CFCS' som tilsynets kontroller, der efter tilsynets opfattelse bør supplere hinanden.

CFCS har taget tilsynets synspunkter til efterretning og tilkendegivet, at centret nærmere vil undersøge, hvorledes CFCS kan efterleve disse.



5

Eksempler på centrets 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 en eller flere konkrete cyberangreb.

Efter drøftelse med tilsynet har CFCS bidraget med følgende beskrivelse af to konkrete cyberangreb:

1. "APT-kampagne via kendte sårbarheder i et open source it-system

Denne case beskriver et vedholdende og bredspektret APT-cyberangreb via kendte sårbarheder i et open source it-system, der bruges i en lang række it-løsninger.

APT står for **Advanced Persistent Threat**. Det er et særligt avanceret, målrettet og vedholdende hacker-angreb. APT-angreb kræver store ressourcer, teknisk indsigt og konkret viden om målet. Angriberne bruger specielle værktøjer, der gør dem i stand til at skjule, at de er til stede i et netværk, og de angriber hyppigt over lang tid. Det er meget sandsynligt, at det er stater eller statsstøttede grupper, der står bag.

CFCS blev gjort opmærksom på en mulig kompromittering af en dansk myndighed af en af FE's partnere. Den pågældende myndighed blev kontaktet af CFCS med henblik på assistance i sagen, og samtidig nedsatte CFCS et såkaldt Incident Response Team. Udrykningsholdet besøgte myndigheden, og det blev bekræftet, at der var malware på den identificerede server. Efter CFCS havde fået samtykke fra myndigheden, blev en kopi af den inficerede server overdraget til CFCS til en såkaldt forensic-analyse.

I de følgende dage blev CFCS bekendt med flere mulige kompromitteringer i Danmark. Disse kompromitteringer blev afdækket som følge af et samarbejde mellem FE, CFCS og fælles partnere; samt som følge af CFCS' egne undersøgelser – herunder i åbne kilder og i CFCS' sensornetværk. I

takt med at ofrene blev identificeret og kontaktet, fik CFCS efter indhentning af samtykke et antal servere ind til undersøgelser. Nye analyser bekræftede, at der også var installeret malware på disse servere. Mindst seks virksomheder og myndigheder blev identificeret som kompromitterede.

Aktøren bag angrebet har udnyttet kendte svagheder i et open source it-system, kaldet JBoss, der anvendes af alle de ramte virksomheder og myndigheder. Manglende opdateringer og fraværet af tilstrækkelig hærdning af it-systemet i overensstemmelse med leverandørens anbefalinger har gjort systemet sårbart. Aktøren bag angrebet har netop udnyttet svaghederne i uopdaterede JBoss-systemer til at installere malware på de ramte maskiner, der giver mulighed for bl.a. at sende kommandoer til maskinen og at få adgang til data, der måtte ligge på den. Under angrebet har aktøren installeret forskellige bagdøre for at få en indledende adgang til serverne og efterfølgende anvendt denne bagdør til at installere en speciel type malware.

Det bemærkes, at JBoss blot er ét blandt mange it-systemer med offentligt kendte svagheder. Alle programmer, der ikke opdateres og hærdes mod cyberangreb, udgør potentielt en lignende sikkerhedsrisiko. CFCS udsendte igennem hele forløbet 23 trusselsvurderinger og varsler om Jboss angreb til virksomheder og myndigheder, der blev vurderet som potentielle brugere med sårbare Jboss-installationer.

På baggrund af egne analyser og understøttet af partnerinformation vurderer CFCS, at det undersøgte angreb er udført af en statslig eller statsstøttet aktør. Det er sandsynligt, at formålet med APT-kampagnen har været opbygning af et ondsindet netværk eller infrastruktur bestående af kompromitterede maskiner til anvendelse i fremtidige cyberangreb.

Grundet JBoss-installationens relative store udbredelse er det meget sandsynligt, at der i dag stadig eksisterer uopdaterede, danske systemer med sårbarheder, der kan udnyttes. Denne case er med til at illustrere de risici, der er forbundet med anvendelsen af uopdaterede open source it-systemer. I denne case indgår der sikkerhedshændelser fra adskillige virksomheder og myndigheder, hvorunder flere kritiske systemer er blevet berørt og hvor system- eller administratorkonti er blevet kompromitteret. På baggrund heraf kategoriserer CFCS på det overordnede plan angrebet i casen som værende et større cyberangreb.

2. Cyberangreb mod danske it-hosting virksomheder

Denne case beskriver et cyberangreb mod to danske it-hosting virksomheder, som er blevet udført i perioden 2015-2016. Begge de ramte it-hostere er mellemstore virksomheder i Danmark, der udbyder forskellige it-løsninger såsom hosting, konsulentbistand, udvikling og drift.

I løbet af 2016 blev CFCS opmærksom på, at de to danske it-hosting virksomheder muligvis kunne være kompromitteret af en statsstøttet aktør. CFCS tog derfor kontakt til de pågældende virksomheder og indhentede samtykke med henblik på at kunne analysere data. På baggrund af angrebenes karakter indledte CFCS' udrykningshold et såkaldt incident response, hvor CFCS indgik et samarbejde med begge virksomheder om analyse og afhjælpning af angrebet. CFCS har således i samarbejde med de to berørte it-hosting virksomheder fundet og analyseret flere kompromitterede maskiner i deres netværk.

Der er fundet to typer APT-malware på de kompromitterede maskiner, og CFCS har kendskab til, at offentlige myndigheder er blandt de to virksomheders kunder. Aktøren har brugt to forskel-

Gate

lige typer malware i sit angreb, der bl.a. kan have været brugt til at fjernstyre kompromitterede maskiner og til at stjæle loginoplysninger eller anden følsom information. Begge typer malware er designet til at gøre dem svære at finde, når de kører på en kompromitteret maskine. Endvidere er dele af deres funktionalitet skjult for at gøre det svært at finde ud af præcis, hvordan de fungerer, hvis de skulle blive fundet alligevel.

Ud over den APT-relaterede malware, er der også fundet flere typer malware, der bruges til almindelig berigelseskriminalitet eller andet misbrug. CFCS' analyse af de kompromitterede computere viser, at aktøren aktivt har forsøgt at skjule sin operation ved at forsøge at slette sine spor. Der er også fundet tegn på, at aktøren har overvåget de kompromitterede maskiner for at se, om angrebet blev opdaget.

CFCS vurderer, at angrebet er gennemført af en statslig eller statsstøttet aktør, muligvis med henblik på at anvende it-hosting virksomhederne som springbræt til data på kundernes netværk, eller med henblik på at sprede malware til senere misbrug.

I perioden 2015-2016 har CFCS observeret, at flere danske it-hosting virksomheder er blevet ramt af cyberangreb, og CFCS har i den forbindelse assisteret de pågældende virksomheder. Denne case er med til at illustrere de risici, der er forbundet med anvendelsen af outsourcet it-drift og anvendelse af eksterne it-services. I denne case indgår der sikkerhedshændelser fra flere forskellige virksomheder og myndigheder, men hvor kritiske systemer ikke er blevet berørt, og hvor system- eller administratorkonti heller ikke er blevet kompromitteret. På baggrund heraf kategoriserer CFCS på det overordnede plan angrebet i casen som værende et moderat cyberangreb."

6 Statistik vedrørende CFCS' behandling af personoplysninger

Af forarbejderne til CFCS-loven fremgår endvidere, at tilsynets årlige redegørelse om sin virksomhed vedrørende CFCS tillige 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 en 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 desuden indeholde en overordnet kategorisering af, hvor alvorlige disse tilfælde har været.

CFCS har efter drøftelse med tilsynet bidraget med følgende data:

Tabel 1 Modtagne klagesager over CFCS' behandling af personoplysninger

Kategorier	2016
Klagesager modtaget i CFCS	0
Klagesager modtaget i tilsynet	0

Tabel 2 Aktindsigtssager

Kategorier	2016
Fuld aktindsigt	1
Delvis aktindsigt	1
Afslag på aktindsigt	0
Ingen dokumenter lokaliseret til at give eller afslå aktindsigt i	1
Total	**3**

Tabel 3 Sager om sikkerhedshændelser, herunder sikkerhedshændelser hvori der er sket indgreb i meddelelseshemmeligheden og foretaget analyse af data, opdelt efter alvorlighed

Kategorier	2016
Alvorlige cyberangreb	0
Større cyberangreb	7
Moderate cyberangreb	24
Mindre cyberangreb	321
Falske positiver (falske alarmer)	413
Åbne sager, der endnu ikke er kategoriseret	18
Total	**783**

Note: Sikkerhedshændelser defineres i overensstemmelse med § 2, nr. 1, i lov om Center for Cybersikkerhed.

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, herunder personoplysninger, der stammer fra indgreb i meddelelseshemmeligheden

Kategorier	2016
Videregivelser	427
Udvekslinger	49

Note: 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 3.1.5.

Appendiks

RETSGRUNDLAG

1) lov om Center for Cybersikkerhed (CFCS) (lovbekendtgørelse nr. 713 af 25. juni 2014) (CFCS-loven).
2) Retningslinjer vedrørende behandling af data i og fra Center for Cybersikkerheds netsikkerhedstjeneste (CFCS-retningslinjerne), udstedt den 30. juni 2014 af Forsvarsministeriet.

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.

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 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. Bestemmelsen er identisk med persondatalovens § 5, stk. 2 og 3, og skal fortolkes i overensstemmelse med denne bestemmelses forarbejder og relevante praksis.

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 persondatalovens § 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).

Bestemmelsens stk. 1 og stk. 2, nr. 1-3, er med sproglige tilpasninger identiske med de tilsvarende bestemmelser i persondatalovens § 7 og skal fortolkes i overensstemmelse med denne bestemmelses forarbejder og relevante praksis. Om stk. 2, nr. 4 og 5, henvises til bemærkningerne ovenfor vedrørende lovens § 10, nr. 4 og 7.

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).

Bestemmelsens stk. 1 og stk. 2, nr. 1-4, er med sproglige tilpasninger identiske med de tilsvarende bestemmelser i persondatalovens § 8 og skal fortolkes i overensstemmelse med disse bestemmelsers forarbejder og relevante praksis. Om bestemmelsens stk. 2, nr. 5, henvises til bemærkningerne ovenfor vedrørende lovens § 10, nr. 7.

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. Bestemmelsen er identisk med den tilsvarende bestemmelse i persondatalovens § 5, stk. 4, og skal fortolkes i overensstemmelse med denne bestemmelses forarbejder og relevante praksis.

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. Bestemmelsen er identisk med den tilsvarende bestemmelse i persondatalovens § 5, stk. 5, og skal fortolkes i overensstemmelse med denne bestemmelses forarbejder og relevante praksis. 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).

4 Om analyse, videregivelse og sletning af data, jf. CFCS-lovens §§ 15-17 og CFCS-retningslinjernes §§ 2, 4, 5 og 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 virksomheders 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 (lovens § 5) er ikke omfattet af lovens § 15, men reguleres nærmere af administrative retningslinjer. Ifølge § 4 i CFCS-retningslinjerne må analyse af pakkedata hidrørende fra netværk hos myndigheder på Forsvarsministeriets område, jf. lovens § 5, kun finde sted

1) ved begrundet mistanke om en sikkerhedshændelse, eller
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, og kun 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, eller
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 informationssikkerhed. 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 (§ 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 meddelelseshemmelighe-

den. 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 tre 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 tre-årige periode igen konstateres anvendt i forbindelse med en sikkerhedshændelse, vil en ny tre-årig 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.

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. Bestemmelsen er indholdsmæssigt identisk med de tilsvarende bestemmelser i persondatalovens § 41, stk. 3 og 4, og skal fortolkes i overensstemmelse med disse bestemmelsers forarbejder og relevante praksis.

Det følger af persondatalovens § 41, stk. 3, at den dataansvarlige skal træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, samt mod at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven, og tilsvarende gælder for databehandlere. Af lovens § 41, stk. 4, fremgår, at der for oplysninger, som behandles for den offentlige forvaltning, og som er af særlig interesse for fremmede magter, skal træffes foranstaltninger, der muliggør bortskaffelse eller tilintetgørelse i tilfælde af krig eller lignende forhold.

Bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning, (sikkerhedsbekendtgørelsen) fastsætter nærmere regler om de i persondatalovens § 41, stk. 3, angivne sikkerhedsforanstaltninger. Uanset at bekendtgørelsen ikke gælder for CFCS' behandling af personoplysninger, har tilsynet ved sin vurdering af kravene til de sikkerhedsforanstaltninger, der følger af CFCS-lovens § 18, henset til bekendtgørelsens bestemmelser, herunder § 5. Af denne bestemmelse følger blandt andet, at den ansvarlige datamyndighed skal fastsætte retningslinjer for myndighedens tilsyn med overholdelse af de sikkerhedsforanstaltninger, der er fastsat af myndigheden, jf. bestemmelsens stk. 1, 4. pkt., og at de interne bestemmelser skal gennemgås mindst én gang hvert år med henblik på at sikre, at de er fyldestgørende og afspejler de faktiske forhold i myndigheden, jf. bestemmelsens stk. 2.

Årsredegørelse 2016
Center for Cybersikkerhed
Udgivet af Tilsynet med Efterretningstjenesterne, maj 2017

Layout + illustrationer: Eckardt ApS
Portrætfotos: Lars Engelgaar

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





Medlemmer af Tilsynet med Efterretningstjenesterne

Landsdommer Ulla Staal, Østre Landsret (formand)
Advokat Pernille Backhausen, Sirius Advokater
Direktør Adam Wolf, Danske Regioner
Professor Jørgen Grønnegård Christensen, Aarhus Universitet
Bestyrelsesformand Erik Jacobsen, Roskilde Universitet

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