Bekendtgørelse af lov om Center for Cybersikkerhed

Ministerium: Forsvarsministeriet	Journalnummer: Forsvarsmin., j.nr. 2019/004062

Bekendtgørelse af lov om Center for Cybersikkerhed

Herved bekendtgøres lov nr. 713 af 25. juni 2014 om Center for Cybersikkerhed med de ændringer, der følger af lov nr. 443 af 8. maj 2018 og lov nr. 555 af 7. maj 2019.

Kapitel 1

Opgaver og organisation

§ 1. Center for Cybersikkerhed har til opgave at understøtte et højt informationssikkerhedsniveau i den informations- og kommunikationsteknologiske infrastruktur, som samfundsvigtige funktioner er afhængige af.

Stk. 2. Center for Cybersikkerhed er en del af Forsvarets Efterretningstjeneste.

Kapitel 2

Definitioner

§ 2. I denne lov forstås ved:

1) Sikkerhedshændelse: En hændelse, der negativt påvirker eller vurderes at ville kunne påvirke tilgængelighed, integritet eller fortrolighed af data, informationssystemer, digitale netværk eller digitale tjenester.
2) Pakkedata: Indholdet af kommunikation, der transmitteres gennem digitale netværk eller tjenester.
3) Trafikdata: Data, som behandles med henblik på at transmittere pakkedata.
4) Stationære data: Data, som opbevares på servere, cloudtjenester, pc'er, lagerenheder, netværksenheder, mobile enheder og tilsvarende.
5) Malware: Trafikdata, pakkedata og stationære data, hvor der er særlig bestyrket mistanke om, at data er anvendt af en angrebsaktør med det formål at forårsage et brud på informationssikkerheden.
6) Personoplysninger: Enhver form for information om en identificeret eller identificerbar fysisk person.
7) Behandling: Enhver operation eller række af operationer med eller uden brug af elektronisk databehandling, som oplysninger gøres til genstand for.

Kapitel 3

Center for Cybersikkerheds netsikkerhedstjeneste

§ 3. Center for Cybersikkerheds netsikkerhedstjeneste har til opgave at opdage, analysere og bidrage til at imødegå sikkerhedshændelser hos tilsluttede myndigheder og virksomheder, jf. stk. 2-4.

Stk. 2. De øverste statsorganer og statslige myndigheder kan efter anmodning blive tilsluttet netsikkerhedstjenesten.

Stk. 3. Regioner og kommuner samt virksomheder, der har samfundsvigtig karakter, kan efter anmodning blive tilsluttet netsikkerhedstjenesten, såfremt Center for Cybersikkerhed konkret vurderer, at tilslutningen vil kunne bidrage til at understøtte et højt informationssikkerhedsniveau i samfundet.

Stk. 4. Center for Cybersikkerhed kan i særlige tilfælde påbyde virksomheder, der har særlig samfundsvigtig karakter, og regioner og kommuner at blive tilsluttet netsikkerhedstjenesten med henblik på monitorering af netværkskommunikation. Påbuddet kan kun omfatte de dele af virksomheden, regionen eller kommunen, der har en væsentlig betydning for Danmarks kritiske infrastruktur. Center for Cybersikkerhed skal mindst hvert halve år vurdere, om et meddelt påbud skal opretholdes.

Stk. 5. Forsvarsministeren kan fastsætte nærmere regler om vilkårene for tilslutning efter stk. 2 og 3. Forsvarsministeren kan desuden fastsætte nærmere regler om påbud efter stk. 4, herunder om, at myndigheder og virksomheder, der er tilsluttet netsikkerhedstjenesten på baggrund af et påbud, skal medvirke til netsikkerhedstjenestens opsætning og drift af hardware og i den forbindelse skal stille

de nødvendige oplysninger om konfiguration og drift af deres digitale infrastruktur til rådighed for netsikkerhedstjenesten.

Kapitel 4

Indgreb omfattet af grundlovens § 72

§ 4. Center for Cybersikkerheds netsikkerhedstjeneste kan uden retskendelse behandle trafikdata, pakkedata og stationære data hidrørende fra tilsluttede myndigheder og virksomheder, jf. § 3, stk. 2-4, med henblik på at understøtte et højt informationssikkerhedsniveau i samfundet.

§ 5. Ved begrundet mistanke om en sikkerhedshændelse kan Center for Cybersikkerheds netsikkerhedstjeneste uden retskendelse behandle stationære data fra en myndighed eller virksomhed, der ikke er tilsluttet netsikkerhedstjenesten, når

1) myndigheden eller virksomheden har anmodet Center for Cybersikkerhed om bistand, stillet de stationære data til rådighed for netsikkerhedstjenesten og givet skriftligt samtykke til behandlingen og
2) behandlingen vurderes at kunne bidrage til at understøtte et højt informationssikkerhedsniveau i samfundet.

§ 6. Efter aftale med en myndighed eller virksomhed, der er tilsluttet Center for Cybersikkerheds netsikkerhedstjeneste i medfør af § 3, stk. 2 og 3, kan netsikkerhedstjenesten ved begrundet mistanke om en sikkerhedshændelse uden retskendelse blokere, omdanne eller omdirigere trafikdata og pakkedata hidrørende fra netværk hos myndigheden eller virksomheden med henblik på at understøtte et højt informationssikkerhedsniveau i samfundet.

Stk. 2. Stk. 1 finder tilsvarende anvendelse i forhold til stationære data hos tilsluttede myndigheder og virksomheder. Ved en konstateret sikkerhedshændelse kan netsikkerhedstjenesten endvidere efter aftale med den tilsluttede myndighed eller virksomhed slette de stationære data, der har forårsaget sikkerhedshændelsen.

§ 6 a. Med henblik på at kunne rådgive myndigheder og virksomheder om forebyggelse af sikkerhedshændelser kan Center for Cybersikkerhed gennemføre forebyggende sikkerhedstekniske undersøgelser, når en myndighed eller virksomhed har anmodet centeret herom.

Stk. 2. Efter anmodning fra myndigheden eller virksomheden kan Center for Cybersikkerhed som led i den forebyggende sikkerhedstekniske undersøgelse

1) uden retskendelse behandle trafikdata, pakkedata og stationære data hos myndigheden eller virksomheden,
2) behandle offentligt tilgængelige data om myndigheden eller virksomheden og dennes medarbejdere og
3) iværksætte forebyggelsesaktiviteter rettet mod udvalgte medarbejdere eller enheder i myndigheden eller virksomheden.

§ 6 b. Med henblik på at opnå viden om angrebsaktørers metoder og værktøjer kan Center for Cybersikkerhed opsætte fiktive angrebsmål, såfremt opsætningen vurderes at kunne bidrage væsentligt til Center for Cybersikkerheds muligheder for at understøtte et højt informationssikkerhedsniveau i samfundet.

Stk. 2. Benytter en angrebsaktør et fiktivt angrebsmål til at deponere data, kan Center for Cybersikkerhed uden retskendelse behandle de deponerede data med henblik på at opdage, analysere og bidrage til at imødegå sikkerhedshændelser hos myndigheder og virksomheder eller at informere borgere, myndigheder og virksomheder om, at de har været udsat for en sikkerhedshændelse.

§ 6 c. Med henblik på at forhindre, standse eller begrænse en nært forestående eller igangværende sikkerhedshændelse kan Center for Cybersikkerhed gøre brug af domænenavne og tilsvarende it-infrastruktur, som anvendes eller har været anvendt af en angrebsaktør, forudsat at disse er ledige til registrering.

Stk. 2. Modtager Center for Cybersikkerhed som led i anvendelsen af it-infrastruktur efter stk. 1 data fra tredjemand, kan centeret uden retskendelse behandle de modtagne data med henblik på at opdage, analysere og bidrage til at imødegå sikkerhedshændelser hos myndigheder og virksomheder eller at informere borgere, myndigheder og virksomheder om, at de har været udsat for en sikkerhedshændelse.

Kapitel 4 a

Edition

§ 7. Med henblik på at afdække sikkerhedshændelser kan der meddeles en juridisk eller fysisk person pålæg om at forevise eller udlevere oplysninger om brugeren af en e-mailkonto, ip-adresse eller et domænenavn, såfremt oplysningerne er undergivet den pågældendes rådighed.

Stk. 2. Pålæg efter stk. 1 må ikke meddeles, såfremt indgrebet står i misforhold til sagens betydning og det tab eller den ulempe, som indgrebet kan antages at medføre.

§ 7 a. Afgørelse om pålæg om edition efter § 7 træffes af retten efter Center for Cybersikkerheds begæring.

Stk. 2. Afgørelsen træffes af retten ved kendelse. Retsmøder holdes for lukkede døre. I kendelsen anføres de konkrete omstændigheder i sagen, hvorpå det støttes, at betingelserne for indgrebet er opfyldt. Kendelsen kan til enhver tid omgøres.

§ 7 b. Inden retten træffer afgørelse om pålæg om edition efter § 7, skal der være givet den, der har rådighed over oplysningerne, adgang til at udtale sig.

Stk. 2. Taler hensynet til fremmede magter eller statens sikkerhed derfor, kan retten eller Center for Cybersikkerhed pålægge den, der har rådighed over oplysninger, som ønskes forevist eller udleveret efter § 7, tavshedspligt med hensyn til den pågældendes viden om sagen. Når pålæg meddeles en erhvervsvirksomhed, gælder dette også for andre juridiske og fysiske personer, der i kraft af deres tilknytning til virksomheden har fået kendskab til sagen.

Stk. 3. Pålæg efter stk. 2 kan ophæves af Center for Cybersikkerhed eller retten. Center for Cybersikkerheds nægtelse af at ophæve et pålæg skal efter begæring forelægges retten. Den pågældende skal gøres bekendt med adgangen hertil.

§ 7 c. Reglerne i retsplejelovens kapitel 63 om værneting og kapitel 85 om kære til højere ret finder tilsvarende anvendelse.

§ 7 d. Center for Cybersikkerhed foranlediger ved at rette henvendelse til den, der har rådighed over oplysningerne, at en kendelse om edition opfyldes. Rettens kendelse skal på begæring forevises den pågældende. Afviser den pågældende uden lovlig grund at efterkomme pålægget, finder reglerne i retsplejelovens § 178 tilsvarende anvendelse.

Kapitel 5

Forholdet til anden lovgivning, behandling af personoplysninger m.v.

§ 8. Center for Cybersikkerheds virksomhed er undtaget fra lov om offentlighed i forvaltningen bortset fra lovens § 13. Center for Cybersikkerheds virksomhed er endvidere undtaget fra forvaltningslovens kapitel 4-6, fra §§ 3 og 5 og § 8, stk. 2, i lov om retssikkerhed ved forvaltningens anvendelse af tvangsindgreb og oplysningspligter og fra databeskyttelsesloven og Europa-Parlamentets og Rådets forordning 2016/679/EU af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger, jf. § 3, stk. 2, i databeskyttelsesloven, og fra lov om retshåndhævende myndigheders behandling af personoplysninger, jf. § 1, stk. 2, i lov om retshåndhævende myndigheders behandling af personoplysninger.

Stk. 2. Forsvarsministeren kan bestemme, at databeskyttelsesloven, Europa-Parlamentets og Rådets forordning 2016/679/EU af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling

af personoplysninger og om fri udveksling af sådanne oplysninger, lov om offentlighed i forvaltningen og forvaltningslovens kapitel 4-6 helt eller delvis finder anvendelse for Center for Cybersikkerhed vedrørende

1) centerets behandling af sager om tilslutning til netsikkerhedstjenesten, jf. § 3, stk. 3 og 4,
2) centerets virksomhed som myndighed for informationssikkerhed og beredskab på teleområdet og
3) centerets personalesager.

Stk. 3. Enhver form for behandling af personoplysninger i Center for Cybersikkerhed er omfattet af kapitel 6. Ved behandling af data, herunder personoplysninger, i medfør af kapitel 4 finder de særlige behandlingsregler i kapitel 7 endvidere anvendelse.

§ 8 a. Oplysninger, der er omfattet af denne lov, kan overføres til opbevaring i arkiv efter reglerne i arkivlovgivningen.

Stk. 2. Forsvarsministeren kan fastsætte nærmere regler om Center for Cybersikkerheds overførsel af oplysninger, der skal bevares for eftertiden, til Rigsarkivet og om centerets opbevaring af sådanne oplysninger, indtil overførsel til Rigsarkivet kan ske.

§ 8 b. Myndigheders og virksomheders samarbejde med Center for Cybersikkerhed er ikke begrænset af bestemmelser om tavshedspligt fastsat ved lov eller med hjemmel i lov, jf. dog stk. 2.

Stk. 2. Forsvarsministeren kan fastsætte regler om, at nærmere angivne bestemmelser om tavshedspligt fastsat ved lov eller med hjemmel i lov fortsat finder anvendelse på myndigheders og virksomheders samarbejde med Center for Cybersikkerhed.

Kapitel 6

Behandling af personoplysninger i Center for Cybersikkerhed

§ 9. Center for Cybersikkerheds indsamling af personoplysninger skal 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.

Stk. 2. 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.

§ 10. Behandling af personoplysninger må 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 Center for Cybersikkerhed eller en tredjemand, til hvem oplysningerne videregives, har fået pålagt,
6) behandlingen er nødvendig for, at Center for Cybersikkerhed 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.

§ 11. Der må ikke behandles personoplysninger om racemæssig eller etnisk baggrund, politisk, religiøs eller filosofisk overbevisning og fagforeningsmæssige tilhørsforhold og personoplysninger om helbredsmæssige og seksuelle forhold.

Stk. 2. Bestemmelsen i stk. 1 finder ikke anvendelse, 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.

§ 12. Der må ikke 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 Center for Cybersikkerheds opgaver.

Stk. 2. De i stk. 1 nævnte personoplysninger må ikke videregives. Videregivelse kan dog ske, hvis

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.

§ 13. Behandling af personoplysninger skal tilrettelægges således, at der foretages fornøden ajourføring af oplysningerne. 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.

§ 14. 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.

Kapitel 7

Analyse, videregivelse og sletning af data

§ 15. Center for Cybersikkerhed kan foretage automatiserede analyser af trafikdata, pakkedata og stationære data, der er omfattet af kapitel 4. Manuelle analyser af data, der er omfattet af kapitel 4, må alene finde sted i følgende tilfælde:

1) For at opdage, analysere og bidrage til at imødegå sikkerhedshændelser kan trafikdata analyseres i det omfang, det er nødvendigt.
2) Ved begrundet mistanke om en sikkerhedshændelse kan pakkedata og stationære data analyseres i det omfang, det er nødvendigt for at afklare forhold vedrørende hændelsen.
3) Som led i forebyggende sikkerhedstekniske undersøgelser efter § 6 a kan trafikdata, pakkedata og stationære data analyseres i det omfang, det er nødvendigt for at gennemføre undersøgelserne.
4) Som led i det løbende arbejde med at understøtte et højt informationssikkerhedsniveau på Forsvarsministeriets område, herunder ved kontrol af, om kommunikation indeholder klassificeret materiale, kan trafikdata og pakkedata, der hidrører fra myndigheder på Forsvarsministeriets område, analyseres.
5) Som led i tekniske test og konfiguration af netsikkerhedstjenestens alarmenheder kan trafikdata og pakkedata analyseres i det omfang, det er nødvendigt for at gennemføre testen. Testen skal afsluttes,

så snart formålet med testen er opfyldt. Analysen må alene foretages af medarbejdere, der varetager tekniske drifts- og udviklingsopgaver for Center for Cybersikkerhed. Øvrige medarbejdere må ikke tilgå oplysninger, der hidrører fra test. Malware, der ved en tilfældighed opdages som led i en teknisk test, må dog analyseres af øvrige medarbejdere i Center for Cybersikkerhed efter nr. 2.

§ 16. Center for Cybersikkerhed kan videregive trafikdata, der er omfattet af kapitel 4, til:

1) Politiet, såfremt der er begrundet mistanke om en sikkerhedshændelse.
2) Den tilsluttede myndighed eller virksomhed, hvorfra de pågældende data hidrører, såfremt der er begrundet mistanke om en sikkerhedshændelse, og hvis det er nødvendigt for udførelsen af Center for Cybersikkerheds opgaver.
3) Danske myndigheder, udbydere af offentlige elektroniske kommunikationsnet og -tjenester og andre netsikkerhedstjenester samt myndigheder og virksomheder i øvrigt i forbindelse med Center for Cybersikkerheds udsendelse af sikkerhedsvarslinger, såfremt der er begrundet mistanke om en sikkerhedshændelse, og såfremt det er nødvendigt for udførelsen af Center for Cybersikkerheds opgaver.

Stk. 2. Center for Cybersikkerhed kan videregive pakkedata, der er omfattet af kapitel 4, til:

1) Politiet, såfremt der er begrundet mistanke om en sikkerhedshændelse.
2) Den tilsluttede myndighed eller virksomhed, hvorfra de pågældende data hidrører, såfremt der er begrundet mistanke om en sikkerhedshændelse.

Stk. 3. Center for Cybersikkerhed kan videregive stationære data, der er omfattet af kapitel 4, til:

1) Politiet, såfremt der er begrundet mistanke om en sikkerhedshændelse.
2) Den myndighed, virksomhed eller borger, hvorfra de pågældende data hidrører, såfremt der er begrundet mistanke om en sikkerhedshændelse.
3) Andre netsikkerhedstjenester, såfremt Center for Cybersikkerhed har modtaget de pågældende data i medfør af § 6 b eller § 6 c.

Stk. 4. Center for Cybersikkerhed kan videregive malware, der er omfattet af kapitel 4, til:

1) Politiet.
2) Den myndighed eller virksomhed, hvorfra de pågældende data hidrører.
3) Danske myndigheder, udbydere af offentlige elektroniske kommunikationsnet og -tjenester og andre netsikkerhedstjenester samt myndigheder og virksomheder i øvrigt i forbindelse med Center for Cybersikkerheds udsendelse af sikkerhedsvarslinger.

Stk. 5. Stk. 1-4 finder ikke anvendelse på data, der stammer fra tekniske test og konfiguration af netsikkerhedstjenestens alarmenheder. Center for Cybersikkerhed kan alene videregive sådanne data i følgende tilfælde:

1) Malware, der er opdaget ved en tilfældighed, kan videregives til politiet, til den myndighed eller virksomhed, hvorfra de pågældende data hidrører, til danske myndigheder, til udbydere af offentlige elektroniske kommunikationsnet og -tjenester og til andre netsikkerhedstjenester samt til myndigheder og virksomheder i øvrigt i forbindelse med Center for Cybersikkerheds udsendelse af sikkerhedsvarslinger.
2) Trafikdata kan videregives til den tilsluttede myndighed eller virksomhed, hvorfra de pågældende data hidrører.

Stk. 6. Uanset stk. 1-4 må Center for Cybersikkerhed i forbindelse med forebyggende sikkerhedstekniske undersøgelser efter § 6 a alene videregive oplysninger vedrørende myndighedens eller virksomhedens medarbejdere, hvis det sker i anonymiseret form.

§ 17. Data, der er omfattet af kapitel 4, slettes, når formålet med behandlingen er opfyldt.

Stk. 2. Uanset at formålet med behandlingen ikke er opfyldt, jf. stk. 1, må

1) data, der knytter sig til en sikkerhedshændelse, højst opbevares i 5 år,

2) data, der ikke knytter sig til en sikkerhedshændelse, men som stammer fra myndigheder, som i særlig grad beskæftiger sig med udenrigs-, sikkerheds- og forsvarspolitiske forhold, samt virksomheder og organisationer, hvis aktiviteter har særlig betydning for disse forhold, højst opbevares i 3 år og
3) øvrige data, der ikke knytter sig til en sikkerhedshændelse, højst opbevares i 13 måneder.

Stk. 3. Fristerne i stk. 2 regnes fra tidspunktet for Center for Cybersikkerheds registrering af de pågældende data.

Stk. 4. Center for Cybersikkerhed kan opbevare backup af data i op til 4 måneder efter udløb af fristerne i stk. 1 og 2. Ved indlæsning af data fra backup skal Center for Cybersikkerhed sikre, at data, der tidligere er slettet efter stk. 1 eller 2, straks slettes igen.

Stk. 5. Er data i medfør af § 16 videregivet til andre end den myndighed eller virksomhed, som data hidrører fra, finder stk. 1 og 2 ikke anvendelse på disse data.

Stk. 6. I data, som Center for Cybersikkerhed får adgang til som led i forebyggende sikkerhedstekniske undersøgelser efter § 6 a, skal personoplysninger, der er indeholdt i disse data, endvidere slettes eller anonymiseres, når den sikkerhedstekniske undersøgelse er afsluttet. Konstaterer Center for Cybersikkerhed, at der i de pågældende data er indeholdt følsomme personoplysninger, skal disse slettes uden unødigt ophold.

Stk. 7. Sletning efter fristerne i stk. 2, nr. 2 og 3, kan i helt særlige tilfælde kortvarigt suspenderes, hvis væsentlige hensyn til varetagelsen af Center for Cybersikkerheds opgaver gør det nødvendigt. Tilsynet med Efterretningstjenesterne skal straks underrettes om suspension efter 1. pkt. og om baggrunden for suspensionen.

§ 17 a. § 17 finder ikke anvendelse på data, der er deponeret på fiktive angrebsmål efter § 6 b eller modtaget via infrastruktur omfattet af § 6 c, såfremt Center for Cybersikkerhed ikke udtager disse data til nærmere vurdering. Disse data slettes hurtigst muligt. Udtager Center for Cybersikkerhed data til nærmere vurdering, skal sletning ske efter reglerne i § 17.

Kapitel 8

Sikkerhedsforanstaltninger

§ 18. Center for Cybersikkerhed træffer 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.

Stk. 2. For oplysninger, som er af særlig interesse for fremmede magter, skal Center for Cybersikkerhed træffe foranstaltninger, der muliggør bortskaffelse eller tilintetgørelse i tilfælde af krig eller lignende forhold.

Kapitel 9

Tilsyn med behandling af personoplysninger

§ 19. Tilsynet med Efterretningstjenesterne, jf. § 16 i lov om Politiets Efterretningstjeneste (PET), fører efter reglerne i dette kapitel tilsyn med Center for Cybersikkerheds behandling af personoplysninger.

Stk. 2. Tilsynet udøver sine funktioner i fuld uafhængighed.

§ 20. Tilsynet påser efter klage eller af egen drift, at Center for Cybersikkerhed overholder reglerne i kapitel 4, 4 a, 6 og 7 vedrørende behandling af personoplysninger.

§ 21. Tilsynet kan som led i sin virksomhed efter § 20 afgive udtalelse over for Center for Cybersikkerhed.

Stk. 2. Tilsynet underretter forsvarsministeren om forhold, som ministeren efter tilsynets opfattelse bør have kendskab til.

Stk. 3. Hvis Center for Cybersikkerhed undtagelsesvis beslutter ikke at følge en henstilling i en udtalelse fra tilsynet, jf. stk. 1, skal centeret underrette tilsynet herom og uden unødigt ophold forelægge sagen for forsvarsministeren til afgørelse.

§ 22. Tilsynet kan hos Center for Cybersikkerhed kræve enhver oplysning og alt materiale, der er af betydning for tilsynets virksomhed.

Stk. 2. Tilsynets medlemmer og sekretariat har til enhver tid mod behørig legitimation uden retskendelse adgang til alle lokaler, hvorfra en behandling, som foretages for Center for Cybersikkerhed, administreres, hvorfra der er adgang til de oplysninger, som behandles, eller hvor tekniske hjælpemidler opbevares eller anvendes.

Stk. 3. Tilsynet kan afkræve Center for Cybersikkerhed skriftlige udtalelser om faktiske og retlige forhold.

Stk. 4. Tilsynet kan anmode om, at en repræsentant for Center for Cybersikkerhed er til stede med henblik på at redegøre for de behandlede sager.

§ 23. Tilsynets virksomhed er undtaget fra lov om offentlighed i forvaltningen bortset fra lovens § 13.

Stk. 2. Tilsynets virksomhed er undtaget fra forvaltningslovens kapitel 4-6 og fra databeskyttelsesloven og fra Europa-Parlamentets og Rådets forordning 2016/679/EU af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og fra lov om retshåndhævende myndigheders behandling af personoplysninger.

§ 24. Tilsynet afgiver en årlig redegørelse om sin virksomhed til forsvarsministeren. Redegørelsen offentliggøres.

Kapitel 9 a

Straffebestemmelser m.v.

§ 24 a. Med bøde straffes, medmindre strengere straf er forskyldt efter den øvrige lovgivning, den, der undlader at efterkomme et pålæg efter § 7 b, stk. 2.

Stk. 2. I regler, der udfærdiges i medfør af § 3, stk. 5, 2. pkt., kan der fastsættes straf i form af bøde for overtrædelse af bestemmelserne i reglerne.

Stk. 3. Der kan pålægges selskaber m.v. (juridiske personer) strafansvar efter reglerne i straffelovens 5. kapitel.

Kapitel 10

Ikrafttrædelses- og overgangsbestemmelser m.v.

§ 25. Loven træder i kraft den 1. juli 2014.

Stk. 2. Lov nr. 596 af 14. juni 2011 om behandling af personoplysninger ved driften af den statslige varslingstjeneste for internettrusler m.v. ophæves.

Stk. 3. Aftaler, der er indgået efter den i stk. 2 nævnte lov, opretholdes, indtil de bortfalder efter deres indhold eller opsiges.

Stk. 4. Loven finder ikke anvendelse på pakke- og trafikdata, der er indsamlet efter den i stk. 2 nævnte lov. For sådanne data finder de hidtil gældende regler anvendelse.

Stk. 5. Loven finder ikke anvendelse på begæringer om aktindsigt, der er indgivet før lovens ikrafttræden. For sådanne begæringer finder de hidtil gældende regler anvendelse.

§ 26. Loven gælder ikke for Færøerne og Grønland, men kan ved kongelig anordning sættes helt eller delvis i kraft for Færøerne og Grønland med de ændringer, som de færøske og grønlandske forhold tilsiger.

Lov nr. 443 af 8. maj 2018 (Konsekvensændringer som følge af databeskyttelsesforordningen og databeskyttelsesloven)[1)] indeholder følgende ikrafttrædelsesbestemmelse:

§ 2

Loven træder i kraft den 25. maj 2018.

Lov nr. 555 af 7. maj 2019 (Initiativer til styrkelse af cybersikkerheden)[2)] indeholder følgende ikrafttrædelsesbestemmelse:

§ 2

Stk. 1. Loven træder i kraft den 1. juli 2019.

Stk. 2. Loven finder ikke anvendelse på data, der er indsamlet før den 1. juli 2019. For sådanne data finder de hidtil gældende regler anvendelse.

Forsvarsministeriet, den 7. august 2019

TRINE BRAMSEN

/ Jon Bach Holm

1) Lovændringen vedrører § 8, stk. 1 og 2, § 14, stk. 2, og § 23, stk. 2.
2) Lovændringen vedrører kapitel 2, § 2, kapitel 3, § 3, kapitel 4, §§ 4-6 c, kapitel 4 a, §§ 7-8 b, § 14, stk. 2, kapitel 7, §§ 15-17 a, § 20, kapitel 9 a og § 24 a.