LOV nr 713 af 25/06/2014 (Historisk)

Lov om Center for Cybersikkerhed

Ministerium: Forsvarsministeriet

Journalnummer: Forsvarsmin., j.nr. 2013/003214

Senere ændringer til forskriften

LOV nr 443 af 08/05/2018 - LOV nr 555 af 07/05/2019 - LBK nr 836 af 07/08/2019

Lov om Center for Cybersikkerhed

VI MARGRETHE DEN ANDEN, af Guds Nåde Danmarks Dronning, gør vitterligt:

Folketinget har vedtaget og Vi ved Vort samtykke stadfæstet følgende lov:

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) *Personoplysninger:* Enhver form for information om en identificeret eller identificerbar fysisk person.
5) *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 myndigheder på Forsvarsministeriets område og hos øvrige tilsluttede myndigheder og virksomheder, jf. stk. 2 og 3.

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

Stk. 3. Regioner og kommuner samt virksomheder, der er beskæftiget med samfundsvigtige funktioner, 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 fastsætte nærmere regler om vilkårene for tilslutning efter stk. 3, herunder regler om betaling af gebyr for tilslutning.

Kapitel 4

Indgreb i meddelelseshemmeligheden

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

§ 5. Center for Cybersikkerheds netsikkerhedstjeneste kan uden retskendelse behandle pakke- og trafikdata hidrørende fra netværk hos myndigheder på Forsvarsministeriets område, jf. § 3, stk. 1, med henblik på at understøtte et højt informationssikkerhedsniveau på området.

§ 6. Ved begrundet mistanke om en sikkerhedshændelse kan en myndighed eller virksomhed, som ikke er tilsluttet Center for Cybersikkerheds netsikkerhedstjeneste efter § 3, midlertidigt 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 Center for Cybersikkerhed om at blive midlertidigt tilsluttet og givet skriftligt samtykke til behandlingen,
2) behandlingen vurderes at kunne bidrage væsentligt til Center for Cybersikkerheds muligheder for at sikre informations- og kommunikationsteknologisk infrastruktur, som samfundsvigtige funktioner er afhængige af, og
3) den midlertidige tilslutning har en varighed på højst 2 måneder.

§ 7. Ved begrundet mistanke om en sikkerhedshændelse kan Center for Cybersikkerheds netsikkerhedstjeneste 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 Center for Cybersikkerhed 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 Center for Cybersikkerheds muligheder for at sikre informations- og kommunikationsteknologisk infrastruktur, som samfundsvigtige funktioner er afhængige af.

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 og fra lov om behandling af personoplysninger, jf. § 2, stk. 11, i lov om behandling af personoplysninger.

Stk. 2. Forsvarsministeren kan bestemme, at kapitel 8-10 i lov om behandling af personoplysninger, lov om offentlighed i forvaltningen og forvaltningslovens kapitel 4-6 helt eller delvis finder anvendelse for Center for Cybersikkerhed vedrørende

1) centerets behandling af anmodninger om tilslutning til netsikkerhedstjenesten, jf. § 3, stk. 3,
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.

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. Analyse af pakkedata, der er omfattet af §§ 4, 6 og 7, må kun finde sted ved begrundet mistanke om en sikkerhedshændelse, og kun i det omfang det er nødvendigt for afklaring af forhold vedrørende hændelsen.

§ 16. Data, der er omfattet af §§ 4, 6 og 7, kan kun videregives i følgende tilfælde:

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

§ 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 3 år og
2) 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. Er data videregivet i medfør af § 16, finder stk. 1 og 2 ikke anvendelse på disse data.

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, 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 lov om behandling af personoplysninger.

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

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.

Givet på Christiansborg Slot, den 25. juni 2014

Under Vor Kongelige Hånd og Segl

MARGRETHE R.

/ Nicolai Wammen