FORSVARSMINISTERIET

Folketingets Forsvarsudvalg
Christiansborg

Dato: 17. april 2019

Enhed: JSN
Sagsnr.: 2019/002204
Dok.nr.: 896992
Bilag: Ingen

FORSVARSMINISTEREN
Holmens Kanal 9
1060 København K

Tlf.: 728 10000
Fax: 728 10300
E-mail: fmn@fmn.dk
www.fmn.dk

EAN: 5798000201200
CVR: 25 77 56 35

Folketingets Forsvarsudvalg har den 3. april 2019 stillet følgende spørgsmål nr. 6 vedrørende L 215, som hermed besvares.

Spørgsmål nr. 6:
"Vil det være muligt at forkorte den periode, hvor Center for Cybersikkerhed opbevarer indsamlet data, før det skal slettes? Herunder bedes forklaret, hvad baggrunden er for perioden på tre år, som er langt længere end den almindelige dataopbevaringsperiode, og om det er nødvendigt, at der er tale om en generel regel for, hvor længe indsamlet data opbevares, fremfor en regel, der kun giver mulighed for en så langvarig dataopbevaring i særlige tilfælde."

Svar:
Det bemærkes indledningsvist, at det følger af § 14 i den gældende lov om Center for Cybersikkerhed, at centeret ikke må opbevare indsamlede personoplysninger 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. Denne bestemmelse foreslås ikke ændret med L 215.

Som supplement til denne generelle sletteregel for personoplysninger gælder der særlige – og mere restriktive – slettefrister for data, der er tilvejebragt på baggrund af indgreb i meddelelseshemmeligheden, herunder bl.a. gennem den monitorering, som Center for Cybersikkerhed foretager hos myndigheder og virksomheder, der er tilsluttet centerets netsikkerhedstjeneste. Disse data skal slettes, når formålet med behandlingen er opfyldt, men derudover er der fastsat absolutte slettefrister, som indebærer, at data skal slettes, når disse absolutte frister udløber – også hvis formålet med behandlingen endnu ikke er opfyldt.

Med lovforslaget foreslås det at udvide den absolutte slettefrist for data i de særlige tilfælde, hvor data er knyttet til en sikkerhedshændelse, fra tre til fem år. Forslaget udspringer af et behov for, at Center for Cybersikkerhed kan bevare viden om tidligere anvendte angrebsmetoder. Ved fastsættelse af den foreslåede tidsgrænse er der endvidere lagt vægt på karakteren af de opbevarede data. Der er således tale om

data, hvor det specifikt er konstateret, at de knytter sig til en sikkerhedshændelse.

Data, der er knyttet til en sikkerhedshændelse, kan f.eks. være en ip-adresse, som har været anvendt ved et cyberangreb mod en dansk myndighed, eller en e-mail-adresse, som har været anvendt til at sende phishing-mails til danske myndigheder. Sådanne data vil især kunne anvendes i netsikkerhedstjenestens monitoreringsudstyr for at give mulighed for, at nye angreb, som kommer fra samme kilde, eller som anvender samme angrebsmetode og -værktøjer, straks kan opdages. Centeret anvender endvidere sin viden om angrebsaktører og angrebsmetoder til at forsøge at være på forkant med nye angrebsmetoder. Selv om angrebsmetoderne løbende udvikler sig, ses det således jævnligt, at tidligere afprøvede teknikker forsøges anvendt på ny. Det ses endvidere ofte, at tidligere anvendte metoder eller delelementer heraf videreudvikles, så de genopstår i nye variationer.

Med den nuværende slettefrist på tre år for data, der er knyttet til en sikkerhedshændelse, er Center for Cybersikkerheds muligheder for at opdage, at angrebsmetoder genanvendes, vanskeliggjort i betydelig grad. Dertil kommer, at sletning af oplysningerne efter tre år vanskeliggør opdagelse af nye variationer af tidligere afprøvede angrebsmetoder. De restriktive betingelser for at opbevare data knyttet til en sikkerhedshændelse har således i en række konkrete tilfælde vist sig at udgøre en betydelig hindring for centerets effektive beskyttelse af samfundsvigtig infrastruktur.

På tilsvarende vis er den nuværende pligt til inden 13 måneder at slette data, der ikke er knyttet til en sikkerhedshændelse, uhensigtsmæssig i de særlige tilfælde, hvor eksempelvis danske myndigheder er genstand for længerevarende angrebskampagner.

Særligt når det gælder opdagelse af avancerede cyberangreb fra statsstøttede aktører har det i forbindelse med alvorlige cyberangreb vist sig at være af meget stor betydning for Center for Cybersikkerhed, at der skabes mulighed for, at centeret kan tilgå ældre data med henblik på at afdække angrebets iværksættelse og varighed, herunder eventuelt identificere andre ofre for samme type angreb. Der vil her være tale om data, som ikke på det pågældende tidspunkt er identificeret som knyttet til en sikkerhedshændelse.

Den foreslåede udvidelse af slettefristen til tre år for data, der ikke er knyttet til en sikkerhedshændelse, vedrører alene data, der hidrører fra en mindre gruppe af myndigheder, som i særlig grad beskæftiger sig med udenrigs-, sikkerheds- og forsvarspolitiske forhold, samt virksom-

heder og organisationer, hvis aktiviteter har særlig betydning for disse forhold.

Det vil eksempelvis dreje sig om udvalgte ministerier og om organisationer, herunder forskningsinstitutioner, der bidrager til den danske udenrigspolitik eller varetager opgaver i den forbindelse, og virksomheder, der leverer materiel og ydelser til Forsvaret.

Der er tale om særligt sensitive data for staten, og det er data, der i særlig grad kan være af interesse for statsstøttede aktører, der spionerer mod Danmark.

Den nuværende slettefrist på 13 måneder i forhold til andre data end de ovennævnte foreslås med lovforslaget videreført uændret.

For så vidt angår data, der ikke er knyttet til en sikkerhedshændelse – det vil sige både data, der fremover omfattes af den særlige slettefrist på tre år og data, der som hidtil er omfattet af slettefristen på 13 måneder – foreslås det dog, at sletning i helt særlige tilfælde kan suspenderes kortvarigt, hvis væsentlige hensyn til varetagelsen af Center for Cybersikkerheds opgaver gør det nødvendigt. I så fald skal Tilsynet med Efterretningstjenesterne straks underrettes, herunder om baggrunden for suspensionen.

På den baggrund vurderes det, at der med de foreslåede slettefrister er fundet en passende balance mellem på den ene side hensynet til retssikkerheden og den personlige frihed og på den anden side hensynet til at styrke Center for Cybersikkerheds muligheder for at opdage og imødegå alvorlige cyberangreb.

Med venlig hilsen

Claus Hjort Frederiksen