Til Forsvarsministeriet (Sag 2018/006599)

KL-svar på høring af forslag til lov om ændring af lov om Center for Cybersikkerhed

Dato: 5. februar 2019

Sags ID: SAG-2019-00318
Dok. ID: 2710582

E-mail: BETR@kl.dk
Direkte: 3370 3064

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

Overordnet mener KL, at lovforslaget og den tilhørende tekst indeholder gode intentioner ift. at give de kommunale myndigheder bedre muligheder i arbejdet med cybersikkerhed.

Dog skal nævnes en bekymring, idet lovforslaget lægger op til, at Center for Cybersikkerheds netsikkerhedstjeneste uden retskendelse kan behandle trafikdata, pakkedata og stationære data hidrørende fra tilsluttede myndigheder og virksomheder med begrundelse om at understøtte et højt informationssikkerhedsniveau. KL er naturligvis ikke bekendt med de trusler, der måtte være, men finder det afgørende, at borgere er trygge ved offentlige myndigheders håndtering af følsomme personoplysninger, hvilket bl.a. også har været bærende for samarbejdet med Sundhedsministeriet om cyberstrategi for sundhedsområdet. Det er KL's opfattelse, at især ønsket om adgang til stationære data kan være med til at svække borgernes tillid til, at følsomme oplysninger, som de har afgivet i f.eks. et behandlingsforløb, vil kunne tilgås af Center for Cybersikkerhed (CFCS) uden hverken medarbejdere eller borgeres viden og uden retskendelse.

Samarbejde på tværs af sektorerne
Forsvarsministeriet lægger op til at øge antallet af myndigheder og virksomheder, der tilsluttes netsikkerhedstjenesten, for at understøtte et højt informationssikkerhedsniveau i den digitale infrastruktur, som samfundsvigtige funktioner er afhængige af. På baggrund af høringsmaterialet er det uklart, i hvilket omfang kommunerne vil blive omfattet, og /eller om det er noget, kommunerne evt. vil skulle anmode om. Det ser ud til, at man også kan blive afvist. Der synes således at være tvivl om kommunernes status ift. det tværgående samarbejde om cybersikkerhed.

I forbindelse med arbejdet med høringen er der opstået tvivl om en række af de juridiske og tekniske forhold omkring det at være tilsluttet netsikkerhedstjenesten. Det er tvivl ift. kommunernes mulighed for risikovurdering af egen it-portefølje, sammenhængen mellem databeskyttelsesloven og evt. udlevering af personoplysninger til CFCS, hvor der er krav, der skal overholdes. Overvejelser om erstatningsansvar, såfremt det er nettjenesten, der er årsag til kompromittering af borgerdata og sammenhængen med Datatilsynets udmeldinger om evt. overtrædelser af meddelelseshemmeligheden, krænkelser af medarbejderes private data mv.

Endelig synes der at være tvivl omkring underretning af bl.a. medarbejdere. Det fremgår både, at medarbejderne hos en myndighed ikke på forhånd bør blive orienteret om, at der gennemføres en sikkerhedsteknisk undersøgelse, end ikke generelt. Der kan orienteres efterfølgende efter aftale med CFCS , men samtidig fremgår det som en del af tilslutningsaftalen mellem CFCS og myndigheden, at der skal ske orientering af medarbejderne om monitoreringen.

Ovenstående synes også umiddelbart at stå i modsætning til Datatilsynets praksis, hvorefter det er den absolutte hovedregel, at de registrerede på forhånd er orienterede om logning og mulig brug heraf. Det er desuden generelt beskrevet som god databehandlingsskik.

KL indgår gerne i dialog om ovenstående. Det har ikke været muligt at behandle lovforslaget politisk, hvorfor der tages forbehold for politisk behandling i KL.

Med venlig hilsen

Pia Færch
Kontorchef
Digitalisering og Teknologi

E-mail: BETR@kl.dk
Direkte: 3370 3064

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk