



JUSTITISMINISTERIET

Administrationsafdelingen

Folketinget
Retsudvalget
Christiansborg
1240 København K

Dato: 26. oktober 2015
Kontor: Koncernstyringskontoret
Sagsbeh: Sidse Hansen Unal
Sagsnr.: 2015-0030-3781
Dok.: 1720908

Hermed sendes besvarelse af spørgsmål nr. 155 (Alm. del), som Folketingets Retsudvalg har stillet til justitsministeren den 3. september 2015. Spørgsmålet er stillet efter ønske fra Lisbeth Bech (SF).

Søren Pind

/

Andreas Langsted

Slotsholmsgade 10
1216 København K.

Telefon 7226 8400
Telefax 3393 3510

www.justitsministeriet.dk
jm@jm.dk

Spørgsmål nr. 155 (Alm. del) fra Folketingets Retsudvalg:

”Mener ministeren, at Datatilsynets anbefalinger i udtalelse af 31. juli 2015 er blevet fulgt til punkt og prikke? Hvis ikke, bedes ministeren redegøre for, hvorfor dette ikke er sket.”

Svar:

Justitsministeriet har til brug for besvarelsen af spørgsmålet indhentet en udtalelse fra Rigspolitiet, der har oplyst følgende:

”Rigspolitiet er den overordnede dataansvarlige for politiets centrale systemer og registre, herunder for de oplysninger der behandles heri. Det er således Rigspolitiets ansvar at sikre, at politiets data behandles sikkerhedsmæssigt forsvarligt – uanset om data ligger hos en ekstern leverandør.

Rigspolitiet er meget opmærksom på de forpligtelser, der følger af dataansvaret. Rigspolitiet tager derfor alle vurderinger og anbefalinger fra Datatilsynet og øvrige myndigheder på området meget alvorligt og inddrager disse i det fortløbende arbejde med datasikkerhed.

Rigspolitiet har således med udgangspunkt i Datatilsynets udtalelse af 31. juli 2015 foretaget en gennemgang af de sikkerhedstiltag, som Rigspolitiet har iværksat i lyset af sikkerhedshændelsen i 2012.

Det er på baggrund af denne gennemgang Rigspolitiets opfattelse, at Rigspolitiet med de iværksatte tiltag har håndteret de kritikpunkter, som Datatilsynet har rejst om sikkerheden på tidspunktet for sikkerhedshændelsen i 2012.

Rigspolitiet har i brev til Datatilsynet af 24. august 2015 orienteret Datatilsynet om de iværksatte sikkerhedstiltag.

Datatilsynet har herefter i brev til Rigspolitiet af 27. august 2015 oplyst, at Datatilsynet på det foreliggende grundlag ikke vil foretage sig yderligere i sagen.

Arbejdet med datasikkerhed er ikke en statisk opgave. Rigspolitiet vil derfor følge den teknologiske udvikling med henblik på løbende at iværksætte relevante forebyggende tiltag i forhold til det aktuelle risikobillede. Rigspolitiet vil desuden i forhold til eksterne driftsleverandører som CSC fremover definere sikkerhedsniveauet og kontrollere efterlevelsen heraf i henhold til anbefalinger fra bl.a. Datatilsynet, Center for Cyber Sikkerhed, PET samt den gældende sikkerhedsstandard (ISO27001)”.

Det kan oplyses, at Datatilsynet – i sin udtalelse af 27. august 2015 – som svar på Rigspolitiets redegørelse af 24. august 2015 har oplyst, at tilsynet har noteret sig Rigspolitiets vurdering af de sikkerhedsmæssige aspekter i forbindelse med en fortsat placering af politiets informationssystemer i det omhandlede mainframemiljø, og at tilsynet i forbindelse med fremtidige inspektioner af Rigspolitiets systemer vil følge op på de rejste sikkerhedsspørgsmål. Datatilsynet har endvidere oplyst, at tilsynet på det foreliggende grundlag ikke foretager sig yderligere i sagen.