JUSTITSMINISTERIET
Politi- og Strafferetsafdelingen

Folketinget
Retsudvalget
Christiansborg
1240 København K

Dato: 30. maj 2017
Kontor: Enheden for Internationalt Politisamarbejde
Sagsbeh: Anne Vibe Bengtsen
Sagsnr.: 2017-0030-5226
Dok.: 2270001

Hermed sendes endelig besvarelse af spørgsmål nr. 295 (Alm. del), som Folketingets Retsudvalg har stillet til justitsministeren den 25. januar 2017. Spørgsmålet er stillet efter ønske fra Søren Søndergaard (EL).

Søren Pape Poulsen

/

Henrik Hjort Elmquist

Slotsholmsgade 10
1216 København K.

T +45 7226 8400
F +45 3393 3510

www.justitsministeriet.dk
jm@jm.dk

Spørgsmål nr. 295 (Alm. del) fra Folketingets Retsudvalg:

> ”Kan ministeren, i forlængelse af samråd den 19. januar 2017 om datalæk i Europol, oplyse, hvordan Europols IT-systemer er opbygget herunder hvilke sikkerhedsstandarder Europol arbejder med, og hvordan det var muligt for en ansat at gemme filer på en privat harddisc, og kan ministeren redegøre for, om og i givet fald hvilke tekniske foranstaltninger Europol har eller vil i værksætte for at undgå, at en enkelt medarbejder fremadrettet kan gemme data på en privat harddisc eller USB-nøgle?”

Svar:

Justitsministeriet har via Rigspolitiet anmodet Europol om oplysninger til brug for besvarelsen af spørgsmålet.

Rigspolitiet har oplyst følgende:

> ”Rigspolitiet har til brug for besvarelsen af spørgsmålet indhentet en udtalelse fra Europol, der bl.a. har oplyst, at Europols informations- og kommunikationsteknologi, herunder Europols operationelle it-system (Operational Network of Europol), er underlagt de højeste sikkerhedsstandarder. Europol har i den forbindelse påpeget, at den omhandlede datalækage ikke var en følge af hacking eller ulovlig indtrængning.
>
> Europol har endvidere oplyst, at Europols systemerne løbende bliver vurderet af Europols Sikkerhedskomité, ligesom de følger en grundig akkrediteringsproces, som også omfatter inddragelse af Europols bestyrelse. Europol har i den forbindelse oplyst, at Operational Network of Europol i oktober 2016 blev opgraderet til klassifikationen ”EU CONFIDENTIAL”.
>
> Herudover har Europol påpeget, at det er syv år siden, at det omhandlede datalækage må antages at have fundet sted, og at dataudtræk fra Europols operationelle it-system i dag er undergivet logningskontrol. Endvidere undervises medarbejdere i Europol løbende i håndteringen af operationelle og følsomme oplysninger. Europol har desuden oplyst, at det siden januar 2017 har været et krav, at enhver ekstern overførsel af data fra Europols operationelle it-system skal godkendes (”4-eye-principle”).
>
> Afslutningsvist har Europol oplyst, at der ikke længere er risiko for et hændelsesforløb svarende til det, der førte til datalækagen, idet det bl.a. ikke længere er muligt at tilslutte private lagringsmedier til Europols computere.”