JUSTITSMINISTERIET

Folketinget
Retsudvalget
Christiansborg
1240 København K
DK Danmark

Dato: 31. august 2018
Kontor: Straffuldbyrdelseskontoret
Sagsbeh: Kristine Toke Mogensen
Sagsnr.: 2018-0030-1285
Dok.: 791472

Hermed sendes endelig besvarelse af spørgsmål nr. 911 (Alm. del), som Folketingets Retsudvalg har stillet til justitsministeren den 22. juni 2018. Spørgsmålet er stillet efter ønske fra Peter Kofod Poulsen (DF).

Søren Pape Poulsen

/

Anders Aagaard

Slotsholmsgade 10
1216 København K.

T +45 7226 8400
F +45 3393 3510

www.justitsministeriet.dk
jm@jm.dk

Spørgsmål nr. 911 (Alm. del) fra Folketingets Retsudvalg:

> ”Vil ministeren redegøre for, hvordan udviklingen af et it-program i det offentlige kan medføre, at et større antal fængselsbetjente har fået lagt deres personfølsomme oplysninger åbent til skue, jf. artiklen ”Politikerne er oprørte over datalæk: »Det er helt katastrofalt«” fra Politiken den 20. juni 2018?”

Svar:

Det er afgørende, at de ansatte i kriminalforsorgen kan have tillid til, at persondata om dem ikke lækkes. Ethvert læk af sådanne oplysninger er selvsagt noget, jeg tager meget alvorligt.

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

> ”Direktoratet for Kriminalforsorgen kan oplyse, at kriminalforsorgen har en kontrakt om support og vedligeholdelse af kriminalforsorgens personalesystem med en it-leverandør. Til at styre disse support- og vedligeholdelsesopgaver anvender leverandøren et sagsstyringsværktøj. Det er i forbindelse med en vedligeholdelsesopgave, at det pågældende datalæk er sket.
>
> Således fik leverandøren i tilknytning til en organisationsændring i kriminalforsorgen i sommeren 2015 til opgave at gennemføre en samlet ændring af personalesystemets såkaldte stamdata. I forbindelse med opgaveløsningen lagde leverandøren oversigten med kriminalforsorgens stamdata ind i sagsstyringsværktøjet.
>
> Efter opgaven var afsluttet, blev oversigten ikke slettet fra leverandørens sagsstyringsværktøj.
>
> Den 20. september 2017 lavede leverandøren en fuld kopi af sagsstyringsværktøjet i forbindelse med en opgradering. Kopien inkluderede al kundedata, der var indeholdt i sagsstyringsværktøjets kundesager. Denne kopi videregav leverandøren til sin underleverandør.
>
> Dette skete uden kriminalforsorgens viden eller godkendelse.
>
> Den 20. december 2017 foretog en medarbejder hos underleverandøren en ændring i den overordnede adgangsstyring til leverandørens sagsstyringsværktøj, og på grund af denne ændring blev der givet fuld adgang til sagsstyringsværktøjets data fra internettet og dermed også til de kundedata, som relaterede sig til kriminalforsorgen.

> Den 1. januar 2018 blev data automatisk indekseret af Google, hvilket er en almindelig rutine fra Google. Den automatiske indeksering medførte, at det herefter var muligt at fremsøge de nævnte stamdata vedrørende kriminalforsorgens personale i leverandørens sagsstyringsværktøj ved hjælp af en Google-søgning.
>
> Leverandøren oplyste den 8. januar 2018, at der var lukket for adgang til leverandørens server og dermed sagsstyringsværktøjer, og at Googles såkaldte cache-version af sagsstyringsværktøjets data var slettet, så det ikke længere var muligt at fremsøge data.
>
> For at imødegå risikoen for lignende hændelser fremover, har kriminalforsorgen under en revision den 6. marts 2018 pålagt den konkrete leverandør at rette op på de uhensigtsmæssigheder, som var observeret i forbindelse med afdækning af hændelsesforløbet.
>
> Kriminalforsorgen har desuden fokus på at forbedre informationssikkerheden, herunder tilsynet med leverandørers håndtering af personoplysninger om såvel medarbejdere som klienter, ligesom der er fokus på, at medarbejdernes bevidsthed om databeskyttelse styrkes.
>
> Erfaringerne fra hændelsesforløbet indgår i det fortsatte arbejde hermed. Kriminalforsorgen vil i den forbindelse bl.a. sikre, at leverandører kun får adgang til live-data, når det er absolut nødvendigt for løsning af en konkret opgave, og at der i sådanne situationer tages de nødvendige sikkerhedsmæssige foranstaltninger."

Justitsministeriet kan desuden henvise til den samtidige besvarelse af spørgsmål 913 (Alm. del) fra Folketingets Retsudvalg, hvoraf det bl.a. fremgår, at kriminalforsorgens undersøgelse af sagen, foretaget med bistand fra PET og et IT-sikkerhedsfirma, viste, at der ikke var tegn på, at andre end kriminalforsorgens medarbejder og Googles indekseringssystem har tilgået oplysningerne.

Justitsministeriet kan afslutningsvist bemærke, at ministeriet i lyset af det generelt skærpede fokus på databeskyttelse har forstærket sin indsats omkring informationssikkerhed. Der er netop ansat en koncerndatadirektør, som sammen med en ny koncerndataenhed skal kortlægge Justitsministeriets hidtidige praksis og compliance vedrørende databeskyttelse mv. På den baggrund skal der fastlægges nye retningslinjer for tilsynet og arbejdet med

databeskyttelse og informationssikkerhed, som sikrer, at Justitsministeriet honorerer de berettigede forventninger om tilstrækkelig beskyttelse af data.