JUSTITSMINISTERIET

Folketinget
Retsudvalget
Christiansborg
1240 København K

Dato: 10. oktober 2017
Kontor: Databeskyttelseskontoret
Sagsbeh: André Dybdal Pape
Sagsnr.: 2017-0030-0204
Dok.: 536041

Hermed sendes besvarelse af spørgsmål nr. 930 (Alm. del), som Folketingets Retsudvalg har stillet til justitsministeren den 12. september 2017.

Søren Pape Poulsen

/

Jakob Lundsager

Slotsholmsgade 10
1216 København K.

T +45 7226 8400
F +45 3393 3510

www.justitsministeriet.dk
jm@jm.dk

Spørgsmål nr. 930 (Alm. del) fra Folketingets Retsudvalg:

> ”I lyset af it-skandalen i Sverige, hvor en leverandør i arbejdet med Transportstyrelsens it-systemer har forbrudt sig i mod den svenske datalov, bedes ministeren redegøre for, hvilke regler og kontrolsystemer der er sat op i Danmark for at undgå det samme?”

Svar:

1. I sommeren 2017 har der været presseomtale i danske medier af en it-skandale i Sverige. Justitsministeriet har i den forbindelse indhentet oplysninger om sagen fra den danske ambassade i Stockholm.

Det fremgår af oplysningerne fra ambassaden, at den svenske sikkerhedsbeskyttelseslov, offentligheds- og fortrolighedslov og personoplysningslov samt interne regler i den svenske transportstyrelse er blevet overtrådt, da den svenske Transportstyrelse i 2015 besluttede at outsource kørsels- og kørekortregistret (inklusive forsvarets og politiets køretøjer) til IBM uden at sikre den nødvendige sikkerhedsgodkendelse af personer og virksomheder, der skulle have adgang til oplysningerne. Herved blev hemmelige svenske registre tilgængelige for ikke-sikkerhedsgodkendt personale i udlandet.

Den svenske sikkerhedsbeskyttelseslov indeholder regler for, hvordan svenske myndigheder skal beskytte sig mod spionage, sabotage, terrorisme eller andre trusler mod rigets sikkerhed.

Den svenske offentligheds- og fortrolighedslov indeholder bestemmelser for myndigheders og visse andre organers håndtering af oplysninger, bestemmelser om tavshedspligt i det offentliges virksomhed og forbud mod at videregive offentlige dokumenter.

Personoplysningsloven i Sverige indeholder regler for myndighedernes behandling af oplysninger om borgerne.

I de omhandlede interne regler i den svenske transportstyrelse er der fastsat bestemmelser for adgang til myndighedens it-systemer og servere.

2.1. For så vidt angår de overordnede rammer for it-sikkerheden hos offentlige myndigheder i Danmark, har Justitsministeriet til brug for besvarelsen

af spørgsmålet indhentet en udtalelse fra Digitaliseringsstyrelsen, der har oplyst følgende:

> ”I henhold til den nationale strategi for cyber- og informationssikkerhed er det obligatorisk for statslige myndigheder at følge standard for informationssikkerhed, ISO27001 (ISO-standarden). Endvidere har kommunerne og regionerne i forbindelse med digitaliseringsstrategien 2016-2020 påtaget sig at følge principperne i ISO-standarden.
>
> ISO-standardens principper skal sikre, at alle it-systemer og -projekter vurderes ud fra en konkret risikovurdering.
>
> Herunder identificeres og klassificeres beskyttelse og håndtering af data i forhold til de lovkrav, generelle såvel som sektorspecifikke, som myndigheden er underlagt, samt reguleringer og anbefalinger. På den baggrund etableres kontrolprocedurer, som er passende for det enkelte system og den enkelte myndighed.
>
> Digitaliseringsstyrelsen er i gang med at gennemføre en modenhedsmåling af arbejdet med ISO27001 i staten. De foreløbige resultater viser, at staten er kommet godt i gang med implementeringen af ISO-standarden.
>
> Modenheden på de helt grundlæggende områder (forretningsoverblik og ledelsesforankring) er betydelig, men der udestår et arbejde for ca. halvdelen af statens myndigheder, når det gælder den resterende del af standarden, herunder fx evaluering af arbejdet med informationssikkerheden og leverandørstyring.
>
> Generelt kræver arbejdet med it-sikkerhed en kontinuerlig indsats af alle myndigheder. Myndighederne skal løbende tilpasse indsatsen i forhold til udviklingen, det gælder fx ændringer i trusselsbilledet og nye teknologiske muligheder.
>
> Digitaliseringsstyrelsen har udviklet et statsligt tilsynskoncept med henblik på at understøtte tilsynet med informationssikkerhedsarbejdet i ministerierne. Konceptet har til formål at sikre, at der føres et systematisk, professionelt og tilbagevendende tilsyn med informationssikkerheden i staten, herunder med fokus på databehandleraftaler og behandling af kritiske informationer.

> Myndighederne skal også stille de rette sikkerhedskrav til it-leverandører og sikre opfølgning på overholdelsen af disse. For at understøtte denne proces har Digitaliseringsstyrelsen udarbejdet et såkaldt klausulbibliotek. Klausulbiblioteket består af en række standardklausuler, der indeholder sikkerhedsmæssige krav rettet mod leverandørerne. Kravene relaterer sig dels til den helt basale håndtering af de omfattede data, dels til efterlevelse af love for deling af og adgange til disse data på tværs af de involverede myndigheder. Formålet med klausulerne er at understøtte myndighedernes arbejde med at stille de korrekte og hensigtsmæssige sikkerhedsmæssige krav ved indgåelse af it-kontrakter."

2.2. Endvidere er det et krav i henhold til retningslinjerne i det såkaldte sikkerhedscirkulære (§ 12), at man skal være sikkerhedsgodkendt, hvis man skal beskæftige sig med klassificerede informationer.

Ifølge sikkerhedscirkulæret (§ 12) må klassificerede informationer ikke gøres tilgængelige for personer, der ikke er sikkerhedsgodkendt til at behandle informationer af den pågældende klassifikationsgrad.

Enhver offentlig myndighed skal træffe afgørelse om sikkerhedsgodkendelse af ansatte i myndigheden og ansatte i private firmaer, der arbejder for den offentlige myndighed. Sikkerhedsgodkendelsen har kun gyldighed for den sikkerhedsgodkendte persons arbejde for den pågældende myndighed.

Behandling af klassificerede informationer må kun betros personer, der er godkendt af vedkommende offentlige myndighed til at behandle informationer af den pågældende klassifikationsgrad.

2.3. Desuden følger det bl.a. af persondataloven, at personer, virksomheder mv., der udfører arbejde for en myndighed, og som får adgang til personoplysninger, kun må behandle disse efter instruks fra myndigheden.

Myndigheden og en eventuel privat leverandør (databehandler) skal ifølge persondataloven træffe fornødne sikkerhedsforanstaltninger mod, at oplysninger bl.a. kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven.

Når en offentlig myndighed overlader en behandling af oplysninger til en databehandler, f.eks. en privat leverandør, skal myndigheden sikre sig og føre tilsyn med, at databehandleren træffer de ovenfor angivne sikkerhedsforanstaltninger.

Den 25. maj 2018 afløses persondataloven af ny generel forordning om databeskyttelse (databeskyttelsesforordningen). Forordningen viderefører i vidt omfang persondatalovens sikkerhedskrav, men indeholder også nye elementer.

Efter databeskyttelsesforordningen skal offentlige myndigheder som noget nyt udpege en databeskyttelsesrådgiver. Formålet med en databeskyttelsesrådgiver er bl.a. at understøtte den dataansvarlige myndigheds sikring af overholdelsen af forordningen. Databeskyttelsesrådgiveren har bl.a. til opgave at overvåge myndighedens overholdelse af regler om databeskyttelse samt underrette og rådgive myndigheden og dens ansatte om deres forpligtelser. Databeskyttelsesrådgiveren skal inddrages i alle spørgsmål vedrørende beskyttelse af personoplysninger hos myndigheden.

Som noget nyt skal der endvidere ske indberetning til Datatilsynet af sikkerhedsbrud. Dette skal ske inden 72 timer.

Regeringen har i forbindelse med finanslovforslaget for finansåret 2018 lagt op til at give Datatilsynet et stort økonomisk løft dels som følge af meropgaver vedrørende databeskyttelsesforordningen mv., dels som en generel styrkelse af Datatilsynet.

Endelig kan det oplyses, at regeringen arbejder på en samlet strategi for beskyttelsen af danskernes personoplysninger.