JUSTITSMINISTERIET

Folketinget
Retsudvalget
Christiansborg
1240 København K
DK Danmark

Dato: 10. marts 2020
Kontor: Databeskyttelseskontoret
Sagsbeh: Mikkel Reenberg
Sagsnr.: 2020-0030-3755
Dok.: 1396703

Hermed sendes besvarelse af spørgsmål nr. 915 (Alm. del), som Folketingets Retsudvalg har stillet til justitsministeren den 12. februar 2020. Spørgsmålet er stillet efter ønske fra Karina Lorentzen Dehnhardt (SF).

Nick Hækkerup

/

Maiken Bøgelund Bek

Slotsholmsgade 10
1216 København K.

T +45 7226 8400
F +45 3393 3510

www.justitsministeriet.dk
jm@jm.dk

Spørgsmål nr. 915 (Alm. del) fra Folketingets Retsudvalg:

> ”Med henvisning til den nylige skandale, hvor 1,2 mio. cpr-numre er blevet lækket fra Tast-Selv Borger til Google og Adobe, samt at der har været flere tidligere data-skandaler hvor f.eks. 5 mio. cpr-numre fra Statens Serum Institut blev sendt til en kinesisk visummyndighed, bedes ministeren besvare følgende:
> a) Vil ministeren redegøre for, hvilke foranstaltninger der findes, for at sikre at danske borgeres data opbevares og behandles sikkert af offentlige myndigheder?
> b) Er ministeren enig i, at et utilstrækkeligt niveau af datasikkerhed medfører en væsentlig risiko for et land med et højt niveau af digitalisering som Danmark?
> c) Hvilke overvejelser har ministeren i forhold til yderligere digitalisering af danske myndigheder, i lyset af at der kan stilles væsentligt spørgsmål ved datasikkerheden?
> d) Vil ministeren redegøre for Datatilsynets kontrol med offentlige myndigheders opbevaring og behandling af borgernes data?
> e) Hvilke initiativer vil ministeren iværksætte, for at sikre at Datatilsynet har tilstrækkelige ressourcer, og at de relevante virkemidler er på plads, til at føre kontrol med offentlige myndigheders databehandling?”

Svar:

Databeskyttelsesreglernes formål er at værne om den enkeltes ret til privatliv. I en tid, hvor vi digitaliserer i udpræget grad i både det offentlige og private, er det særligt vigtigt, hvordan vi beskytter vores oplysninger.

I et moderne digitaliseret samfund vil det unægtelig være sådan, at der er større risiko for, at vores oplysninger kommer uvedkommende til kendskab, end hvis vi levede i et samfund, hvor computere og andet teknisk udstyr ikke var en del af dagligdagen.

Men jeg mener ikke, at vi som samfund skal undgå at digitalisere som følge af en generel frygt for, at vores oplysninger kommer uvedkommende i hænde.

Derimod skal vi sikre, at digitalisering sker så det altid sikres, at håndteringen af vores oplysninger foregår på en betryggende måde. Databeskyttelsesreglerne er med til at sikre netop dette.

Med de nye databeskyttelsesregler fra 2018 er der kommet større opmærksom omkring, hvordan offentlige myndigheder og private aktører håndterer

personoplysninger. Det samme gælder mulighederne for at pålægge sanktioner, hvor der f.eks. nu er mulighed for, at offentlige myndigheder straffes med bøde for overtrædelse af reglerne. Det kan eksempelvis udgøre en overtrædelse, hvis der ikke er tilstrækkelig sikkerhed omkring håndteringen af personoplysninger. Jeg henviser til Datatilsynets bidrag nedenfor, hvor der er redegjort nærmere for tilsynets reaktionsmuligheder.

For så vidt angår Datatilsynets ressourcer blev tilsynet med finansloven for 2018 styrket med 12,5 mio. kr. i 2018, 16,4 mio. kr. i 2019 og 16,8 mio. kr. i 2020 og frem, dels som følge af meropgaver vedrørende databeskyttelsesforordningen mv., dels som en generel styrkelse af Datatilsynet. Det er således som udgangspunkt min opfattelse, at Datatilsynet har de nødvendige ressourcer.

Justitsministeriet har til brug for besvarelsen af spørgsmålets punkt a og d indhentet en udtalelse fra Datatilsynet. Hvad angår punkt a oplyser Datatilsynet følgende:

> "Når en offentlig myndighed behandler personoplysninger finder databeskyttelsesforordningen og databeskyttelsesloven anvendelse, jf. forordningens artikel 2, stk. 1 og lovens § 1, stk. 2.
>
> Enhver behandling af personoplysninger skal således ske under iagttagelse af reglerne i databeskyttelsesforordningen, databeskyttelsesloven og eventuelle særregler, som ligger inden for databeskyttelsesforordningens rammer for særregler om behandling af personoplysninger.
>
> Det følger bl.a. af databeskyttelsesforordningen, at myndigheder, der behandler oplysninger om borgere, skal påse, at behandlingen af personoplysninger har en passende sikkerhed, jf. navnlig artikel 32. Udgangspunktet er således, at der ved behandling af personoplysninger skal gennemføres passende tekniske og organisatoriske foranstaltninger for at sikre fysiske personers rettigheder og frihedsrettigheder. Ved vurderingen af, hvad der er passende, skal der bl.a. tages hensyn til den pågældende behandlings karakter og formål samt risiciene for fysiske personers rettigheder og frihedsrettigheder.
>
> En væsentlig del af vurderingen af niveauet for behandlingssikkerhed er personoplysningernes karakter, herunder om der er tale om oplysninger af fortrolig eller følsom karakter.
>
> Passende tekniske og organisatoriske foranstaltninger kan eksempelvis være test af systemer og behandlinger, isolation af brugeradgange, kryptering af personoplysninger, systemovervågning, logning af brugere, overordnet brugerstyring og lø-

bende uddannelse og træning af medarbejdere i databeskyttelsesreglerne."

Hvad angår spørgsmålets punkt d, oplyser Datatilsynet følgende:

"Efter databeskyttelseslovens § 27, stk. 1, fører Datatilsynet tilsyn med overholdelsen af de generelle databeskyttelsesregler, der findes i databeskyttelsesforordningen, databeskyttelsesloven og anden lovgivning, som ligger inden for databeskyttelsesforordningens rammer for særregler om behandling af personoplysninger. Datatilsynet har bl.a. til opgave at behandle klager, der indgives af registrerede, ligesom tilsynet af egen drift – bl.a. i form af ad hoc tilsyn – påser, om behandling af personoplysninger finder sted i overensstemmelse med navnlig databeskyttelsesforordningen og databeskyttelsesloven. Datatilsynet orienterer sig i den forbindelse løbende i sager debatteret i medierne mv. med henblik på at vurdere, om der bør indledes undersøgelser på tilsynets eget initiativ.

Det er efter Datatilsynets opfattelse afgørende for at sikre en høj beskyttelse af danskernes personoplysninger – og derfor også tilsynets vision – at myndigheder kender og overholder reglerne for behandling af personoplysninger, og at borgerne kender og kan bruge deres rettigheder. Datatilsynet gør dette muligt og lettere gennem synlighed, information, dialog og kontrol. Det er samtidig Datatilsynets mission at rådgive om registrering, videregivelse og anden behandling af personoplysninger og føre tilsyn med, at myndigheder og andre dataansvarlige overholder reglerne på området.

Af databeskyttelseslovens § 29 fremgår det, at Datatilsynet kan kræve enhver oplysning, der er af betydning for tilsynets virksomhed, herunder til afgørelse af, om et forhold falder ind under databeskyttelsesforordningens og lovens bestemmelser. Datatilsynet har endvidere beføjelse til at få adgang til alle lokaler, hvorfra en behandling af personoplysninger foretages. Politiet kan i fornødent omfang bistå Datatilsynet hertil.

Hvis der sker en overtrædelse af databeskyttelsesreglerne, herunder f.eks. reglerne om behandlingssikkerhed, har Datatilsynet en række reaktionsmuligheder. Det følger af databeskyttelsesforordningens artikel 58, stk. 2, at tilsynet har beføjelse til:

a) at udstede advarsler til en dataansvarlig eller en databehandler om, at planlagte behandlingsaktiviteter sandsynligvis vil være i strid med denne forordning
b) at udtale kritik af en dataansvarlig eller en databehandler, hvis behandlingsaktiviteter har været i strid med denne forordning

c) at give den dataansvarlige eller databehandleren påbud om at imødekomme den registreredes anmodninger om at udøve sine rettigheder i henhold til denne forordning
d) at give den dataansvarlige eller databehandleren påbud om at bringe behandlingsaktiviteter i overensstemmelse med bestemmelserne i denne forordning og, hvis det er hensigtsmæssigt, på en nærmere angivet måde og inden for en nærmere angivet frist
e) at give den dataansvarlige påbud om at underrette den registrerede om et brud på persondatasikkerheden
f) midlertidigt eller definitivt at begrænse, herunder forbyde, behandling
g) at give påbud om berigtigelse eller sletning af personoplysninger eller begrænsning af behandling i henhold til artikel 16, 17 og 18 og meddelelse af sådanne handlinger

Overtrædelse af databeskyttelsesreglerne kan efter omstændighederne således sanktioneres ved bl.a. at udtale kritik og/eller meddele den dataansvarlige påbud eller forbud i forhold til en given handling eller undladelse. Efter omstændighederne kan det også komme på tale at sanktionere overtrædelsen med en bøde. De forskellige sanktioner kan enten anvendes alene eller kombineres afhængigt af de konkrete omstændigheder.

Ifølge databeskyttelseslovens § 41, stk. 6, 2. pkt., kan offentlige myndigheder og institutioner – uanset straffelovens § 27, stk. 2, – straffes for overtrædelse af databeskyttelsesforordningen og -loven i fuldt omfang. Det betyder, at offentlige myndigheder også kan straffes, selv om der ikke er tale om virksomhed, som kan sidestilles med virksomhed udøvet af private.

Justitsministeriet har i de almindelige bemærkninger til lovforslaget til databeskyttelsesloven forudsat, at bødelofterne for alle offentlige myndigheder, er lavere end dem, der fremgår af forordningens artikel 83, stk. 4-6. Bødelofterne er herefter:

- For overtrædelser omfattet af forordningens artikel 83, stk. 4: 2 % af myndighedens driftsbevilling, dog maksimalt 8.000.000 kroner
- For overtrædelser omfattet af forordningens artikel 83, stk. 5 og 6: 4 % af myndighedens driftsbevilling, dog maksimalt 16.000.000 kroner

Det fremgår endvidere af bemærkningerne, at der ved pålæggelse af bøder til offentlige myndigheder skal tages hensyn til, at de – i modsætning til private aktører – efter lovgivningen er pålagt at varetage lovbestemte opgaver, og at myndigheder derfor heller ikke uden videre i alle tilfælde blot kan standse en behandling for derved at bringe en eventuel ulovlig tilstand til op-

hør. Der skal endvidere lægges vægt på myndighedernes rammevilkår, som for nogle kan betyde, at de har en bevilling, der er bundet tæt op på deres lovbundne opgave.

Datatilsynet kan oplyse, at tilsynet i 2019 har afsluttet mere end 6.500 sager, herunder forespørgsler, klager, tilsyn og sikkerhedsbrud, vedrørende offentlige myndigheders behandling af personoplysninger."