



JUSTITSMINISTERIET

Folketinget
Kulturudvalget
Christiansborg
1240 København K
DK Danmark

Dato: 15. juni 2021
Kontor: Databeskyttelseskontoret
Sagsbeh: Anna Skovrup
Sagsnr.: 2021-0032/14-0045
Dok.: 1992475

Besvarelse af spørgsmål nr. 316 (Alm. del) fra Folketingets Kulturudvalg

Hermed sendes besvarelse af spørgsmål nr. 316 (Alm. del), som Folketingets Kulturudvalg har stillet til justitsministeren den 20. maj 2021. Spørgsmålet er stillet efter ønske fra Morten Messerschmidt (DF).

Nick Hækkerup

/

Mie Vinkel Sørensen

Slotsholmsgade 10
1216 København K.

T +45 3392 3340
F +45 3393 3510

www.justitsministeriet.dk
jm@jm.dk

Spørgsmål nr. 316 (Alm. del) fra Folketingets Kulturudvalg:

”Mange virksomheder udsteder billetter mv. til deres kunder, hvorved billetten giver adgang til den konkrete oplevelse. Det gælder eksempelvis på teatre, i biografer, forlystelsesparker og andet. For nogle virksomheder er det afgørende, at billetten ikke kan overdrages. I den forbindelse er det relevant at få afklaret, hvorvidt der i den aktuelle lovgivning findes hindringer for, at en virksomhed - med kundens samtykke - må bruge ansigtsscan og – genkendelse I stedet for billet/adgangskort. Vil ministeren på den baggrund oplyse, hvilke regler gælder for brug af ansigtsgenkendelse som adgangsgivende billet/kort i en privat virksomhed, og er der hindringer i lovgivningen for, at en virksomhed, der normalt udstyrer sine medarbejdere med kort til åbning af døre og lignende i stedet gøre brug af ansigtsgenkendelse/scan?”

Svar:

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

”Af databeskyttelsesforordningens¹ artikel 9, der omhandler særlige kategorier af personoplysninger – ofte benævnt følsomme personoplysninger – følger af bestemmelsens stk. 1, at behandling af personoplysninger om bl.a. biometriske data med henblik på entydig identifikation er forbudt. Ved biometriske data forstås f.eks. ansigtsbillede eller fingeraftryksoplysninger.

Det står ikke Datatilsynet klart, hvilken teknisk løsning der nærmere sigtes til, og tilsynet kan derfor ikke vurdere, i hvilket omfang behandlingen af oplysninger er omfattet af artikel 9, stk.1, om behandling af følsomme oplysninger.

Hvis der er tale om en løsning, hvor der sker *sammenligning* af oplysninger om en persons ansigt (indsamlet på tidspunktet for identifikation) med en række biometriske skabeloner, som er lagret i en database, således at der sker en eller flere matchprocesser, vil behandlingen af oplysningerne være omfattet af artikel 9, stk. 1, idet der vil være tale om behandling af personoplysninger med henblik på entydig identifikation.

¹ Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse).

Personoplysninger omfattet af forbuddet i artikel 9, stk. 1, må kun behandles, hvis en af undtagelserne i artikel 9, stk. 2, litra a-j, finder anvendelse. I den pågældende situation vil det umiddelbart være relevant at overveje artikel 9, stk. 2, litra a og g:

- a) Den registrerede har givet udtrykkeligt samtykke til behandling af sådanne personoplysninger til et eller flere specifikke formål, medmindre det i EU-retten eller medlemsstaternes nationale ret er fastsat, at det i stk. 1 omhandlede forbud ikke kan hæves ved den registreredes samtykke.
- g) Behandling er nødvendig af hensyn til væsentlige samfundsinteresser på grundlag af EU-retten eller medlemsstaternes nationale ret og står i rimeligt forhold til det mål, der forfølges, respekterer det væsentligste indhold af retten til databeskyttelse og sikrer passende og specifikke foranstaltninger til beskyttelse af den registreredes grundlæggende rettigheder og interesser.

Enhver behandling af personoplysninger kræver endvidere, at den dataansvarlige har et lovligt behandlingsgrundlag i databeskyttelsesforordningens artikel 6, stk. 1, litra a-f. Dette gælder tillige, hvis der er tale om behandling af oplysninger, som ikke er omfattet af artikel 9, stk. 1, om følsomme oplysninger.

Det følger af databeskyttelsesforordningens artikel 6, stk. 1, at personoplysninger kan behandle, hvis:

- a) Den registrerede har givet samtykke til behandling af sine personoplysninger til et eller flere specifikke formål.
- b) Behandling er nødvendig af hensyn til opfyldelse af en kontrakt, som den registrerede er part i, eller af hensyn til gennemførelse af foranstaltninger, der træffes på den registreredes anmodning forud for indgåelse af en kontrakt.
- c) Behandling er nødvendig for at overholde en retlig forpligtelse, som påhviler den dataansvarlige.
- d) Behandling er nødvendig for at beskytte den registreredes eller en anden fysisk persons vitale interesser.
- e) Behandling er nødvendig af hensyn til udførelse af en opgave i samfundets interesse eller som henhører under offentlig myndighedsudøvelse, som den dataansvarlige har fået pålagt.
- f) Behandling er nødvendig for, at den dataansvarlige eller en tredjemand kan forfølge en legitim interesse, medmindre den registreredes interesser eller grundlæggende rettigheder og frihedsrettigheder, der kræver beskyttelse af personoplysninger, går forud herfor, navnlig hvis den registrerede er et barn.

I det omfang behandling af personoplysninger skal ske på grundlag af samtykke efter databeskyttelsesforordningens artikel 9, stk. 2, litra a eller artikel 6, stk. 1, litra a, forudsætter det, at samtykket, som den registrerede skal give, er frivilligt, specifikt, informeret og udtryk for en utvetydig viljestilkendegivelse, jf. databeskyttelsesforordningens artikel 4, stk. 1, nr. 11. Kravet om frivillighed indebærer, at den registrerede skal have et reelt eller frit valg og skal kunne trække sit samtykke tilbage, uden at det i øvrigt er til skade for den pågældende.

Det er efter Datatilsynets opfattelse umiddelbart tvivlsomt, om et samtykke til behandlingen af oplysninger i den beskrevne situation kan anses for frivilligt, medmindre den registrerede tilbydes en alternativ mulighed for identifikation, hvis vedkommende ikke ønsker at give samtykke til brug af ansigtsgenkendelse.

Datatilsynet har tidligere behandlet en sag om adgangskontrol i Tivoli vedrørende brug af en billeddatabase i forbindelse med adgangskontrol til Tivoli². Datatilsynet vurderede, at behandlingen af billederne kunne ske på baggrund af samtykke, og tilsynet lagde i den forbindelse netop vægt på, at Tivolis kunder havde mulighed for at vælge andre løsninger ved besøg i Tivoli. Det bemærkes, at afgørelsen er truffet efter de tidligere regler i persondataloven, og at der ikke ved behandlingen var tale om anvendelse af biometriske data med henblik på entydig identifikation, hvorfor behandlingen ikke angik følsomme oplysninger, ligesom løsningen ikke anvendte automatisk ansigtsgenkendelse, men en manuel håndtering af billeder af årskortholdere.

Personoplysninger kan endvidere under visse betingelser behandles, hvis behandlingen er nødvendig af hensyn til væsentlige samfundsinteresser, jf. artikel 9, stk. 2, litra g, og artikel 6, stk. 1, litra e.

Hvis en privat dataansvarlig ønsker at behandle følsomme oplysninger på grundlag af artikel 9, stk. 2, litra g, skal Datatilsynet give tilladelse til behandlingen, jf. databeskyttelseslovens § 7, stk. 4³. Ved en anmodning om tilladelse vurderer tilsynet bl.a. særligt, om behandlingen er nødvendig af hensyn til en væsentlig samfundsmæssig interesse.

² Datatilsynets udtalelse kan findes på tilsynets hjemmeside: <https://www.datatilsynet.dk/afgoerelser/historiske-afgoerelser/2006/jan/billeddatabase-i-forbindelse-med-adgangskontrol>.

³ Lov nr. 502 af 23. maj 2018 om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesloven).

Datatilsynet har givet tilladelse til behandling af biometriske data ved brug af automatiske ansigtsgenkendelsessystemer efter databeskyttelseslovens § 7, stk. 4⁴. Sagen omhandlede Brøndby Stadion, som ønskede at etablere adgangskontrol ved indgangene til stadionet ved brug af automatisk ansigtsgenkendelse med henblik på at identificere personer, som var på deres karantæneliste for at undgå uroligheder på stadion og dermed øge sikkerheden for tilskuerne.

Hvis behandlingen af oplysninger i den omtalte løsning ikke indebærer behandling af følsomme oplysninger, kan behandlingen finde sted, hvis den dataansvarlige har et behandlingsgrundlag i artikel 6, stk. 1, og de grundlæggende principper for behandling af personoplysninger er opfyldt.

Den dataansvarlige skal overveje, hvilket behandlingsgrundlag, der eventuelt kan finde anvendelse ved behandlingen efter databeskyttelsesforordningens artikel 6, stk. 1. I den forbindelse skal den dataansvarlige vurdere, om behandling ved brug af ansigtsgenkendelse kan anses for at være nødvendig i den omhandlede sammenhæng.

Behandling af personoplysninger skal desuden generelt ske under iagttagelse af de grundlæggende principper i forordningens artikel 5, herunder princippet om dataminimering.

Princippet om dataminimering indebærer, at behandlingen af personoplysninger ikke må gå videre end, hvad der kræves for at opfylde de formål, som den dataansvarlige er berettiget til at forfølge. Den dataansvarlige bør derfor altid overveje om en behandling af personoplysninger er nødvendig for at opfylde formålet, herunder om det er proportionalt, dvs. om formålet kan opnås ved brug af mindre indgribende metoder.

Datatilsynet skal afslutningsvist bemærke, at tilsynet ikke ses at have haft sager vedrørende den omhandlede problemstilling, og således ikke har haft anledning til at tage stilling hertil.”

2. Justitsministeriet har endvidere til brug for besvarelsen af spørgsmålet indhentet en udtalelse fra Erhvervsministeriet, der har oplyst følgende:

”Brugen af kunstig intelligens til blandt andet ansigtsgenkendelse er derudover kommet på dagsordenen i EU, hvor Europa-Kommissionen (Kommissionen) har fremlagt et forslag til for-

⁴ Tilladelsen kan findes på Datatilsynets hjemmeside: <https://www.datatilsynet.dk/afgoerrelser/tilladelser/2019/maj/tilladelse-tilbehandling-af-biometriske-data-ved-brug-af-automatisk-ansigtsgenkendelse-ved-indgange-paa-broendby-stadion>

ordning om harmoniserede regler for kunstig intelligens. Forslaget har blandt andet til formål at sikre, at kunstig intelligens, der markedsføres og anvendes i EU, er sikker og respekterer eksisterende lovgivning, grundlæggende rettigheder samt EU's værdier.

Kommissionens forslag følger en risikobaseret tilgang, hvor graden af forpligtelser følger graden af de risici, der er forbundet med den pågældende anvendelse af kunstig intelligens. Anvendelsen af systemer til realtidsfjernbiometrisk identifikation af personer, hvilket vil omfatte ansigtsgenkendelse, anses af Kommissionen for at udgøre en høj risiko for individers grundlæggende rettigheder. Af den grund pålægges denne anvendelse en række forpligtelser i forslaget, herunder blandt andet i forhold til data og forvaltning, journalføring, gennemsigtighed og levering af information til brugerne, menneskeligt tilsyn samt nøjagtighed, robusthed og cybersikkerhed. Kommissionen foreslår, at efterlevelsen af kravene sikres gennem en forudgående overensstemmelsesvurdering samt en løbende kontrol heraf.

Teknologien er i hastig udvikling, men der foreligger ikke et konkret overblik over danske virksomheders anvendelse af ansigtsgenkendelse til brug for adgangsgivende billet/kort.”