DATATILSYNET

Justitsministeriet
Slotsholmsgade 10
1216 København K
Danmark

Sendt med Digital Post

18. maj 2021

J.nr. 2020-442-10939
Dok.nr. 350298
Sagsbehandler
Poul Erik Weidick

Datatilsynet
Carl Jacobsens Vej 35
2500 Valby
T 3319 3200
dt@datatilsynet.dk
datatilsynet.dk

CVR 11883729

Vedrørende brud på persondatasikkerheden

Datatilsynet vender hermed tilbage til sagen, hvor Justitsministeriet den 14. december 2020 har anmeldt et brud på persondatasikkerheden til Datatilsynet. Anmeldelsen har følgende referencenummer:

bad9cb6a554f3bdb8f37c834e60179b5dbb40114.

1. Afgørelse

Efter en gennemgang af sagen finder Datatilsynet, at der er grundlag for at udtale **alvorlig kritik** af, at Justitsministeriets behandling af personoplysninger ikke er sket i overensstemmelse med reglerne i databeskyttelsesforordningens[1] artikel 32, stk. 1, og artikel 33, stk. 1.

Nedenfor følger en nærmere gennemgang af sagen og en begrundelse for Datatilsynets afgørelse.

2. Sagsfremstilling

Justitsministeriet har den 14. december 2020 anmeldt et brud på persondatasikkerheden til Datatilsynet. Af anmeldelsen fremgår, at Justitsministeriet den 28. januar 2020 modtog en redegørelse fra Rigspolitiet om en fangeflugt fra et psykiatrisygehus den 19. november 2019. Det fremgik af redegørelsen, at den var udarbejdet til brug for offentliggørelse og blev derfor offentliggjort på Justitsministeriets og Folketingets hjemmesider den 3. februar 2020.

Forsvarsadvokaten for den undvegne fange klagede den 28. februar 2020 til Justitsministeriet over offentliggørelsen, idet den indeholdt følsomme personoplysninger i form af helbredsoplysninger, ligesom den indeholdt oplysninger om strafbare forhold, der ikke havde været offentligt tilgængelige forud for offentliggørelse af redegørelsen.

Justitsministeriet behandlede sagen, bl.a. i form af en høring til Rigspolitiet, men blev først opmærksom på, at sagen skulle indberettes som et brud på persondatasikkerheden den 11. december 2020, hvorefter, der straks blev iværksat sletning af redegørelsen fra de hjemmesider, hvor den var offentliggjort.

[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).

3. Justitsministeriets oplysninger

Justitsministeriet har til sagen oplyst, at Justitsministeriet den 28. januar 2020 modtog en redegørelse fra Rigspolitiet om en fangeflugt den 19. november 2019 fra et psykiatrisygehus. Redegørelsen blev offentliggjort på Justitsministeriets hjemmeside den 3. februar 2020 og offentliggjort på Folketingets hjemmeside samme dag. Redegørelsen blev udarbejdet af Rigspolitiet med bidrag fra Direktoratet for Kriminalforsorgen, Rigsadvokaten og Region Sjælland efter anmodning fra Justitsministeriet om en redegørelse til brug for offentliggørelse. Det fremgik derfor også af redegørelsen, at den var udarbejdet til brug for offentliggørelse.

Da Justitsministeriet den 28. februar 2020 modtog en klage fra den undvegne indsattes forsvarsadvokat over, at den offentliggjorte redegørelse indeholdt følsomme personoplysninger i form af helbredsoplysninger, iværksatte ministeriet en høring af Rigspolitiet den 3. marts 2020 med henblik på at få afklaret, hvorvidt og i givet fald i hvilket omfang redegørelsen efter Rigspolitiets opfattelse indeholdt følsomme personoplysninger.

I høringssvar af 12. maj 2020 tilsluttede Rigspolitiet sig advokatens opfattelse af, at redegørelsen indeholdt følsomme personoplysninger i form af helbredsoplysninger. Rigspolitiet konstaterede endvidere, at redegørelsen indeholdt oplysninger om den pågældendes strafbare forhold, som ikke var offentligt tilgængelige forud for offentliggørelse af redegørelsen. Rigspolitiet konkluderede, at de pågældende oplysninger ikke var egnet til offentliggørelse.

De relevante fagkontorer i Justitsministeriets departement var hverken ved modtagelsen af advokatens henvendelse den 28. februar 2020 eller ved modtagelsen af Rigspolitiets høringssvar den 12. maj 2020 opmærksomme på, at sagen skulle håndteres som et brud på persondatasikkerheden. Der blev derfor ikke taget skridt til at få fjernet redegørelsen fra Justitsministeriets hjemmeside og Folketingets hjemmeside, ligesom sagen ikke blev forelagt Justitsministeriets databeskyttelsesrådgiver (DPO) eller sikkerhedsofficer med henblik på anmeldelse af bruddet til Datatilsynet.

Justitsministeriet blev først opmærksom på, at sagen skulle behandles som en brud på persondatasikkerheden den 11. december 2020 i forbindelse med udarbejdelse af svar på forsvarsadvokatens klage, hvor Justitsministeriets Databeskyttelseskontor og DPO blev inddraget i sagen. Redegørelsen blev samme dag fjernet fra Justitsministeriets hjemmeside, ligesom ministeriet tog kontakt til Folketingets Udvalgssekretariat, hvorefter redegørelsen også blev fjernet fra Folketingets hjemmeside henholdsvis den 11. december 2020 (fra Retsudvalgets offentliggjorte dokumenter) og den 14. december 2020 (fra Sundheds- og Ældreudvalgets offentliggjorte dokumenter).

I overensstemmelse med departementets interne procedure for håndtering af brud på persondatasikkerheden blev Justitsministeriets sikkerhedsofficer den 14. december 2020 underrettet om sagen med henblik på anmeldelse af bruddet til Datatilsynet. Sagen blev anmeldt til Datatilsynet samme dag. Det har ikke været muligt at afdække nærmere, hvorfor sagen ikke tidligere i forløbet er blevet håndteret korrekt.

Justitsministeriet har videre anført, at den aktuelle hændelse, som skyldes menneskelige fejl, viser, at der er behov for, at ministeriet revurderer indholdet af sine uddannelses- og awarenessindsatser med fokus på at skærpe medarbejdernes viden og opmærksomhed omkring beskyttelse af personoplysninger, herunder brud på persondatasikkerheden. Ministeriet vil derfor gennemgå indholdet af de beskrevne uddannelses- og awarenessindsatser med henblik på at sikre, at de i videst muligt omfang imødekommer dette behov. Derudover er Justitsministeriet i gang med at udarbejde en politik om beskyttelse af personoplysninger med henblik på at styrke databeskyttelsen i departementets sagsbehandlingsprocesser. Dette arbejde forventes færdigt i 1. halvår 2021. Endelig har Justitsministeriet som følge af hændelsen fun-

det anledning til at indskærpe vigtigheden af fokus på databeskyttelse over for ministeriets underliggende myndigheder, herunder betydningen af at alle myndigheder selvstændigt bidrager til databeskyttelsen på tværs af koncernen.

4. Begrundelse for Datatilsynets afgørelse

Datatilsynet lægger på baggrund af det af Justitsministeriet den 3. marts 2021 oplyste til grund, at ministeriet den 3. februar 2020 – som følge af menneskelige fejl – har offentliggjort en af Rigspolitiet udfærdiget redegørelse om en fangeflugt fra et psykiatrisygehus den 19. november 2019. Redegørelsen indeholdt oplysninger om den flygtede fanges helbred og oplysninger om ikke tidligere offentliggjorte strafbare forhold. Herudover lægges det efter det oplyste ligeledes til grund, at der i det offentliggjorte var personoplysninger, der ikke skulle have været inkluderet i teksten.

Datatilsynet lægger på den baggrund til grund, at der ved offentliggørelsen er sket en ulovlig videregivelse af personoplysninger, hvorfor tilsynet finder, at der er sket et brud på persondatasikkerheden, jf. databeskyttelsesforordningens artikel 4, nr. 12.

4.1. Databeskyttelsesforordningens artikel 32

Det følger af databeskyttelsesforordningens artikel 32, stk. 1, at den dataansvarlige skal træffe passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til de risici, der er ved den dataansvarliges behandlinger af personoplysninger.

Der påhviler således den dataansvarlige en pligt til at identificere de risici, den dataansvarliges behandling udgør for de registrerede og til at sikre, at der indføres passende sikkerhedsforanstaltninger, der beskytter de registrerede mod disse risici.

Det er Datatilsynets opfattelse, at kravet jf. artikel 32 om passende sikkerhed normalt vil indebære, **at** man som dataansvarlig sikrer, at oplysninger om registrerede, herunder især følsomme oplysninger, ikke kommer til uvedkommendes kendskab og **at** der bør stilles højere krav til medarbejdernes omhyggelighed i tilfælde hvor personoplysninger skal offentliggøres, herunder skal der ved en gennemgang af materialet foretages sikring af, at der ikke sker uautoriseret offentliggørelse af beskyttelsesværdige eller følsomme personoplysninger.

Det er Datatilsynets vurdering, at Justitsministeriet som minimum skulle have gennemgået dokumentet og vurderet, om der af dette fremgik oplysninger, der efter gældende regler ikke kunne offentliggøres. Ved ikke at gøre dette har Justitsministeriet overtrådt databeskyttelsesforordningens artikel 32 om passende sikkerhed.

Datatilsynet har noteret sig, at Justitsministeriet forud for hændelsen har implementeret en række organisatoriske foranstaltninger med henblik på undgå brud på persondatasikkerheden og at ministeriet efter hændelsen har revurderet disse foranstaltninger og arbejder med at skærpe medarbejdernes viden og opmærksomhed omkring beskyttelse af personoplysninger.

4.2. Databeskyttelsesforordningens artikel 33

Det følger af forordningens artikel 33, stk. 1, at den dataansvarlige i tilfælde af brud på persondatasikkerheden uden unødig forsinkelse og om muligt inden 72 timer skal foretage anmeldelse af bruddet til Datatilsynet, medmindre at det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder.

Det fremgår af sagen, at Justitsministeriet den 28. februar 2020 modtog en klage over redegørelsens offentliggørelse fra den registreredes forsvarsadvokat. Justitsministeriet iværksatte den 3. marts 2020 en høring af Rigspolitiet med henblik på at få afklaret, hvorvidt og i givet fald i hvilket omfang den offentliggjorte redegørelse efter Rigspolitiets opfattelse indeholdt føl-

somme personoplysninger. Allerede på dette tidspunkt burde Justitsministeriet have overvejet og vurderet om der forelå et brud på databeskyttelsesforordningen, der skulle indberettes til Datatilsynet.

Da Justitsministeriet den 12. maj 2020 modtog Rigspolitiets høringssvar, hvoraf det fremgik, at Rigspolitiet vurderede, at redegørelsen indeholdt oplysninger, der ikke var egnet til offentliggørelse, burde Justitsministeriet have indset, at der var tale om et brud på persondatasikkerheden og indberettet dette til Datatilsynet.

Datatilsynet finder, at Justitsministeriets behandling af personoplysninger – ved først at anmelde bruddet den 11. december 2020 – ikke er sket i overensstemmelse med databeskyttelsesforordningens artikel 33, stk. 1.

4.3. Sammenfatning

På ovenstående baggrund finder Datatilsynet, at der samlet set er grundlag for at udtale **alvorlig kritik** af, at Justitsministeriets behandling af personoplysninger ikke er sket i overensstemmelse med reglerne i databeskyttelsesforordningens artikel 32, stk. 1, og artikel 33, stk. 1.

Datatilsynet har ved valg af reaktion lagt vægt på, at personoplysningerne omfattede helbredsoplysninger og oplysninger om ikke tidligere offentliggjorte strafbare forhold.

Samtidig er det Datatilsynets opfattelse, at der henset til Justitsministeriets arbejdsområder og funktion, kan stilles højere krav til, at vurderinger efter de gældende regler herunder databeskyttelsesreglerne foretages korrekt. Dette gælder særligt vurderingen af hvilke oplysninger der skal ekstraheres inden oplysninger offentliggøres. Herudover burde Justitsministeriet allerede ved modtagelsen af klagen fra den registreredes advokat, have vurderet om der var forhold der skulle ekstraheres, og allersenest ved modtagelsen af Rigspolitiets redegørelse den 12. maj 2020, have ageret i overensstemmelse med den vurdering, der fremgik heraf. Det er således skærpende, at ministeriet først ca. 7 måneder senere reagerer herpå, og tager skridt til at slette oplysningerne, og på dette senere tidspunkt, får anmeldt forholdet til Datatilsynet.

5. Afsluttende bemærkninger

Datatilsynet bemærker, at Datatilsynets afgørelse ikke kan indbringes for anden administrativ myndighed, jf. databeskyttelseslovens § 30.

Datatilsynets afgørelse kan dog indbringes for domstolene, jf. grundlovens § 63.

Datatilsynet anser hermed sagen for afsluttet og foretager sig herefter ikke yderligere i sagen.

Med venlig hilsen

Poul Erik Weidick

Bilag: Retsgrundlag.

Bilag: Retsgrundlag

Uddrag af 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).

Artikel 2, stk. 1. Denne forordning finder anvendelse på behandling af personoplysninger, der helt eller delvis foretages ved hjælp af automatisk databehandling, og på anden ikkeautomatisk behandling af personoplysninger, der er eller vil blive indeholdt i et register.

Artikel 4. I denne forordning forstås ved:

1) »personoplysninger«: enhver form for information om en identificeret eller identificerbar fysisk person (»den registrerede«); ved identificerbar fysisk person forstås en fysisk person, der direkte eller indirekte kan identificeres, navnlig ved en identifikator som f.eks. et navn, et identifikationsnummer, lokaliseringsdata, en onlineidentifikator eller et eller flere elementer, der er særlige for denne fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sociale identitet
2) »behandling«: enhver aktivitet eller række af aktiviteter — med eller uden brug af automatisk behandling — som personoplysninger eller en samling af personoplysninger gøres til genstand for, f.eks. indsamling, registrering, organisering, systematisering, opbevaring, tilpasning eller ændring, genfinding, søgning, brug, videregivelse ved transmission, formidling eller enhver anden form for overladelse, sammenstilling eller samkøring, begrænsning, sletning eller tilintetgørelse

[…]

7) »dataansvarlig«: en fysisk eller juridisk person, en offentlig myndighed, en institution eller et andet organ, der alene eller sammen med andre afgør, til hvilke formål og med hvilke hjælpemidler der må foretages behandling af personoplysninger; hvis formålene og hjælpemidlerne til en sådan behandling er fastlagt i EU-retten eller medlemsstaternes nationale ret, kan den dataansvarlige eller de specifikke kriterier for udpegelse af denne fastsættes i EU-retten eller medlemsstaternes nationale ret

[…]

12) »brud på persondatasikkerheden«: et brud på sikkerheden, der fører til hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet

Artikel 32. Under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder gennemfører den dataansvarlige og databehandleren passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til disse risici, herunder bl.a. alt efter hvad der er relevant:

a) pseudonymisering og kryptering af personoplysninger
b) evne til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester
c) evne til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse
d) en procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed.

Stk. 2. Ved vurderingen af, hvilket sikkerhedsniveau der er passende, tages der navnlig hensyn til de risici, som behandling udgør, navnlig ved hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.

Stk. 3. Overholdelse af en godkendt adfærdskodeks som omhandlet i artikel 40 eller en godkendt certificeringsmekanisme som omhandlet i artikel 42 kan bruges som et element til at påvise overholdelse af kravene i nærværende artikels stk. 1.

Stk. 4. Den dataansvarlige og databehandleren tager skridt til at sikre, at enhver fysisk person, der udfører arbejde for den dataansvarlige eller databehandleren, og som får adgang til personoplysninger, kun behandler disse efter instruks fra den dataansvarlige, medmindre behandling kræves i henhold til EU-retten eller medlemsstaternes nationale ret.

Artikel 33. Ved brud på persondatasikkerheden anmelder den dataansvarlige uden unødig forsinkelse og om muligt senest 72 timer, efter at denne er blevet bekendt med det, bruddet på persondatasikkerheden til den tilsynsmyndighed, som er kompetent i overensstemmelse med artikel 55, medmindre at det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder. Foretages anmeldelsen til tilsynsmyndigheden ikke inden for 72 timer, ledsages den af en begrundelse for forsinkelsen.

Stk. 2. Databehandleren underretter uden unødig forsinkelse den dataansvarlige efter at være blevet opmærksom på, at der er sket brud på persondatasikkerheden.

Stk. 3. Den i stk. 1 omhandlede anmeldelse skal mindst:

a) beskrive karakteren af bruddet på persondatasikkerheden, herunder, hvis det er muligt, kategorierne og det omtrentlige antal berørte registrerede samt kategorierne og det omtrentlige antal berørte registreringer af personoplysninger
b) angive navn på og kontaktoplysninger for databeskyttelsesrådgiveren eller et andet kontaktpunkt, hvor yderligere oplysninger kan indhentes
c) beskrive de sandsynlige konsekvenser af bruddet på persondatasikkerheden
d) beskrive de foranstaltninger, som den dataansvarlige har truffet eller foreslår truffet for at håndtere bruddet på persondatasikkerheden, herunder, hvis det er relevant, foranstaltninger for at begrænse dets mulige skadevirkninger.

Stk. 4. Når og for så vidt som det ikke er muligt at give oplysningerne samlet, kan oplysningerne meddeles trinvist uden unødig yderligere forsinkelse.

Stk. 5. Den dataansvarlige dokumenterer alle brud på persondatasikkerheden, herunder de faktiske omstændigheder ved bruddet på persondatasikkerheden, dets virkninger og de trufne afhjælpende foranstaltninger. Denne dokumentation skal kunne sætte tilsynsmyndigheden i stand til at kontrollere, at denne artikel er overholdt.