DATATILSYNET

AROS Privathospital Partnerselskab
Skejbyparken 154
8200 Aarhus N

Sendt med Digital Post

25. november 2020

J.nr. 2019-41-0037
Dok.nr. 239925
Sagsbehandler
Nicklas Irgens Høj
Villien

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

CVR 11883729

Tilsyn med anmeldelse af brud på persondatasikkerheden

AROS Privathospital Partnerselskab var blandt de private virksomheder, som Datatilsynet i foråret 2019 havde udvalgt at føre tilsyn med efter databeskyttelsesforordningen[1] og databeskyttelsesloven[2].

Datatilsynets tilsyn var et skriftligt tilsyn, som navnlig fokuserede på, om AROS Privathospital Partnerselskab foretager anmeldelse af brud på persondatasikkerheden i overensstemmelse med databeskyttelsesforordningens artikel 33, stk. 1, og om privathospitalet opfylder kravet om at dokumentere alle brud på persondatasikkerheden, jf. artikel 33, stk. 5.

AROS Privathospital Partnerselskab har endvidere i forbindelse med tilsynet efter anmodning fra Datatilsynet generelt redegjort for privathospitalets uddannelse af medarbejdere – i forhold til håndteringen af brud på persondatasikkerheden – med henblik på, at privathospitalet kan iagttage databeskyttelsesforordningens artikel 33.

Datatilsynets tilsyn blev ved brev af 11. marts 2019 varslet over for AROS Privathospital Partnerselskab, og privathospitalet blev ved samme lejlighed anmodet om bl.a. at besvare en række spørgsmål.

Ved brev af 13. marts 2019 sendte AROS Privathospital Partnerselskab en udtalelse, hvor privathospitalet i tilknytning til svarene på Datatilsynets spørgsmål oplyste, at privathospitalet ikke har registrerede brud på persondatasikkerheden i perioden fra 25. maj 2018 til og med 8. marts 2019. AROS Privathospital Partnerselskabs svar var endvidere vedlagt to dokumenter om hospitalets håndtering af persondata, som privathospitalet anvender for at efterleve artikel 33 i databeskyttelsesforordningen.

1. Afgørelse

Henset til, at AROS Privathospital Partnerselskab i den pågældende periode ikke har registret brud på persondatasikkerheden, og idet tilsynet ikke har fundet indikationer på, at dette skulle være sket, har Datatilsynet fundet, at privathospitalet har iværksat de foranstaltninger, der er nødvendige for at kunne overholde kravene i databeskyttelsesforordningens artikel 33, stk. 1,

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)
2 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)

og derved sikre, at brud på persondatasikkerheden opfanges i organisationen og registreres, sådan at disse altid bliver vurderet med henblik på om bruddet skal anmeldes til Datatilsynet.

Datatilsynet har på det foreliggende grundlag vurderet, at AROS Privathospital Partnerselskab samlet set har levet op til kravene i databeskyttelsesforordningens artikel 33, stk. 5.

Det er herudover Datatilsynets vurdering, at AROS Privathospital Partnerselskab har gennemført passende uddannelsesaktiviteter bl.a. med henblik på at kunne understøtte identifikation og håndtering af brud på persondatasikkerheden.

Nedenfor følger en nærmere gennemgang af de oplysninger, der er kommet frem i forbindelse med tilsynet og en begrundelse for Datatilsynets afgørelse.

2. Anmeldelse af brud på persondatasikkerheden

Et brud på persondatasikkerheden er i databeskyttelsesforordningens artikel 4, nr. 12, defineret som 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.

Det følger endvidere af databeskyttelsesforordningens artikel 33, stk. 1, at ved brud på persondatasikkerheden skal den dataansvarlige uden unødig forsinkelse og om muligt senest 72 timer, efter at den dataansvarlige er blevet bekendt med bruddet på persondatasikkerheden anmelde dette 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, skal den ledsages af en begrundelse for forsinkelsen.

AROS Privathospital Partnerselskab har i privathospitalets udtalelse af 13. marts 2019 til Datatilsynet oplyst, at der i perioden fra 25. maj 2018 til og med 8. marts 2019 ikke er registreret hændelser, der er kategoriseret som egentlige *brud på persondatasikkerheden,* jf. databeskyttelsesforordningens artikel 4, nr. 12.

Datatilsynet har ikke fundet indikationer på, at der har været hændelser der burde have været anmeldt, og har derfor ved tilsynet fundet, at AROS Privathospital Partnerselskab har levet op til kravet om, at alle relevante brud på persondatasikkerheden er blevet anmeldt til Datatilsynet, jf. databeskyttelsesforordningens artikel 33, stk. 1.

Samlet set har Datatilsynet derfor ikke fundet grundlag for at konkludere, at AROS Privathospital Partnerselskab har registreret informationssikkerhedshændelser, herunder brud på persondatasikkerheden, som burde have været anmeldt til Datatilsynet, men som ikke er blevet det.

3. Dokumentation af brud på persondatasikkerheden

Ifølge databeskyttelsesforordningens artikel 33, stk. 5, skal den dataansvarlige dokumentere 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 (Datatilsynet) i stand til at kontrollere, at bestemmelsen er overholdt.

Det bemærkes, at der stilles ikke specifikke formkrav til dokumentationen, og den dataansvarlige kan derfor selv beslutte, hvordan oplysningerne skal indsamles, og hvordan de skal præsenteres. Dokumentationen skal imidlertid i alle tilfælde indeholde en række informationer, jf.

bestemmelsens ordlyd ovenfor. I Datatilsynets vejledning fra februar 2018 om håndtering af brud på persondatasikkerheden er på side 27 anført, at kravene til dokumentation kan opstilles således:

- Dato og tidspunkt for bruddet
- Hvad skete der i forbindelse med bruddet?
- Hvad er årsagen til bruddet?
- Hvilke (typer) personoplysninger er omfattet af bruddet?
- Hvilke konsekvenser har bruddet for de berørte personer?
- Hvilke afhjælpende foranstaltninger er truffet?
- Hvorvidt – og i givet fald hvordan – der er sket anmeldelse til Datatilsynet? Hvorfor/Hvorfor ikke?

Den dataansvarlige bør således dokumentere sine begrundelser for alle væsentlige beslutninger, der træffes som følge af bruddet. Dette gælder ikke mindst, hvis den dataansvarlige, efter at have vurderet bruddet, er nået frem til, at det ikke skal anmeldes til Datatilsynet.

AROS Privathospital Partnerselskab har i forbindelse med tilsynet oplyst, at privathospitalet ikke har oplevet et brud på persondatasikkerheden. Privathospitalet har således ikke været i besiddelse af materiale, der kunne dokumentere håndteringen af brud. Datatilsynet har ikke fundet indikationer på hændelser der burde have været anført.

På baggrund af den fremsendte dokumentation, er det Datatilsynets vurdering, at AROS Privathospital Partnerselskab samlet set har levet op til kravene i databeskyttelsesforordningens artikel 33, stk. 5.

4. Uddannelse af medarbejdere

Det fremgår af databeskyttelsesforordningens artikel 32, stk. 1, at den dataansvarlige skal gennemføre passende tekniske og organisatoriske foranstaltninger for at sikre et passende sikkerhedsniveau.

Heraf kan bl.a. udledes krav om, at den dataansvarlige skal sikre sig, at alle medarbejdere i organisationen i nødvendigt omfang er bekendt med eventuelle interne procedurer for håndtering af brud på persondatasikkerheden, at visse relevante medarbejdere kan identificere og vurdere brud på persondatasikkerheden, herudover er det en nødvendighed for at organisationen som helhed i øvrigt er i stand til at understøtte forpligtelsen til at foretage indberetninger mv. i medfør af databeskyttelsesforordningens artikel 33.

Datatilsynet har noteret sig, at AROS Privathospital Partnerselskab har oplyst, at der har været afholdt to aktiviteter med henblik på at uddanne alle hospitalets medarbejdere i at kunne identificere og håndtere brud på persondatasikkerheden.

Datatilsynet har ikke haft lejlighed til at tage konkret stilling til, om alle relevante medarbejdere har gennemført de pågældende uddannelsesaktiviteter, og tilsynet er ikke er bekendt med det anvendte uddannelsesmateriale Det er dog tilsynets opfattelse, at de aktiviteter der er udført er egnede som passende uddannelsesaktiviteter bl.a. med henblik på at kunne understøtte identifikation og håndtering af brud på persondatasikkerheden. Efter omstændighederne, særligt at der ikke er indikationer på brud og det i øvrigt i sagen belyste, har tilsynet fundet oplysningsniveauet passende

5. Sammenfatning

Henset til, at AROS Privathospital Partnerselskab i perioden, ikke har registret brud på persondatasikkerheden, og idet tilsynet ikke har fundet indikationer på, at dette skulle være sket,

har Datatilsynet fundet, at privathospitalet har iværksat de foranstaltninger, der er nødvendige for at kunne overholde kravene i databeskyttelsesforordningens artikel 33, stk. 1, og derved sikre, at brud på persondatasikkerheden opfanges i organisationen og registreres, sådan at disse altid bliver vurderet med henblik på om bruddet skal anmeldes til Datatilsynet.

Datatilsynet har på det forligende grundlag vurderet, at AROS Privathospital Partnerselskab samlet set har levet op til kravene i databeskyttelsesforordningens artikel 33, stk. 5.

Det er herudover Datatilsynets vurdering, at AROS Privathospital Partnerselskab har gennemført passende uddannelsesaktiviteter bl.a. med henblik på at kunne understøtte identifikation og håndtering af brud på persondatasikkerheden.

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

Det skal for god ordens skyld oplyses, at Datatilsynet – i en nyhed på tilsynets hjemmeside – den 2. december 2020 forventer at offentliggøre navnene og eventuelle sanktioner på de institutioner, offentlige myndigheder og private virksomheder, der har været omfattet af dette tilsyn.

Med venlig hilsen

Allan Frank