DATATILSYNET

Familieretshuset
Storetorv 10
6200 Aabenraa

6. september 2022

J.nr. 2021-432-0063
Dok.nr. 507117
Sagsbehandler
Betty Husted

Sendt med Digital Post

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

CVR 11883729

Familieretshusets utilsigtede videregivelser af oplysninger om beskyttet navn og adresse

Datatilsynet vender hermed tilbage til sagen, hvor tilsynet på baggrund af en række anmeldte brud på persondatasikkerheden den 13. oktober 2021 startede en sag af egen drift vedrørende Familieretshusets utilsigtede videregivelser af beskyttede navne- og adresseoplysninger.

Datatilsynet har efterfølgende modtaget yderligere anmeldelser fra Familieretshuset om lignende hændelser.

Anmeldelserne omfattet af denne afgørelse er modtaget fra den 27. maj 2021 til den 16. august 2022 og har følgende referencenumre:

1. cc4946f11f4a6fe895ffff75c6f86013413cfe61
2. add576ddae85727c50a947fbdca51977dadf3d8a
3. b02ba0b2a15d4673bb8757aec0d5426039b053ae
4. ea195b4a6303a794024f943b780a7bcc53e4e237
5. 5bb123241e708622c749354f6bf0aa974b50a85a
6. a4e04c590badc8453e5c023b019497d0743706af
7. f4dee9d5bf57d506aecb781f920e23df4addef42
8. f146fd3f2e73e8493bc5f84a4a466b003336d54c
9. b4b0ee6e8b050c9308981a99a37a360f528f2be5
10. 58b192f6b1a3047211075e3c421b3a911a57de7e
11. b792255bf814cc17ae9e485c8d241c98b1d2002c
12. 61500d8c6b3f59a11fc45ed718fb3fa6458cc899
13. 7540b3eaafb691d49aa2deb860038d4a74e48880
14. 827eb25c94b5b9f7a560a90243a37f1084640e09
15. 8b6bea72535bd51d08827a318f94dc9f600223fd
16. bb1fe9af77fd15c3c364222fd2ab0ca328a99a77
17. ff7566c450bdaafb02902e9f29f9bf544745ff52
18. 0d22de8e31322991a9a7aa9325369cb218f2f978
19. 8215604b5b223b529a78b2c09edb188426349a10
20. 9d0c697862f16692d45bd4d873767d359ee37da3
21. 5d32b522d3bcb98de1c280f1c101f95276f874f1
22. d9b7de23e27d7a130b28eaa753d6b1357f57119a
23. 0aabdfad36c1ff4404374702e6ab18adcebad495
24. 58e9e2f1546fa2764e19fb04d09762a9bcdd64ba

25. 3747311bdc31fd84c228deac21055ad00dae9913
26. f11a0bdc939250493e1ca770599636aa5536325a
27. 3fed056166be823c8c500bb5f5c0851c1267ec2c
28. f6c00d55c772601ab47f9d030f86092f3869cf22
29. d27f36404e1605d766d9e933834e35a5081a3a84
30. a35c2950c5227b94158b2cbff847648f3d62213a
31. caae132d30cb2a60799c04fe7444c95b78f383d6
32. abef532eb5283b45a488047af14b8ec3b430fca3
33. 50931c16d015399b88a95a9a9d84639059b52ab1
34. 7b8b12110dfa170e11bd641b207cd378b2b710c6
35. 2b76dd6614d4642eec90a01aea94139eecede9fb
36. 51d65c63671a2be351eae2c3638e468ec5122bd7
37. 8350634c78402b3b962d7022f5228e2d43c729b9

Bruddet med referencenummer d9b7de23e27d7a130b28eaa753d6b1357f57119a blev oprindeligt afsluttet den 1. juli 2021 med et afsluttende brev. Det fremgår imidlertid af brevet, at Datatilsynet – typisk hvis der måtte fremkomme nye oplysninger eller klager i sagen, eller hvis tilsynet modtager nye anmeldelser om brud på persondatasikkerheden fra Familieretshuset – vil kunne genoptage sagen eller lade den indgå i vurderingen af eventuelle fremtidige brud – eller klagesager. Det pågældende brud er derfor også omfattet af denne afgørelse.

Datatilsynet startede den 1. oktober 2020 en sag af egen drift over for Familieretshuset, da tilsynet kunne konstatere, at Familieretshuset frem til den 27. september 2020 havde anmeldt 158 brud på persondatasikkerheden, og at 130 af disse anmeldelser vedrørte utilsigtet videregivelse af personoplysninger. Datatilsynet traf den 4. marts 2021 afgørelse i sagen. Datatilsynet fandt bl.a., at Familieretshuset ikke i tilstrækkelig grad havde sikret, at medarbejderne havde haft den fornødne omhu ved behandling af borgernes personoplysninger, herunder beskyttede navne- og adresseoplysninger.

Det var Datatilsynets vurdering, at de menneskelige fejl kunne være undgået under iagttagelse af fornøden omhu fra medarbejdernes side, ligesom den ekstra kontrol, der blev udført af en anden sagsbehandler, åbenbart ikke var tilstrækkelig effektiv. Datatilsynet udtalte også, at Familieretshuset samtidig burde indføre effektive tekniske kontrolforanstaltninger ved fremsendelse af sagsbehandlingsdokumenter via elektronisk post, således at disse dokumenter ikke ved en fejl blev sendt til uvedkommende.

Datatilsynet fandt på ovenstående baggrund, at der var grundlag for at udtale alvorlig kritik af, at Familieretshusets behandling af personoplysninger ikke var sket i overensstemmelse med reglerne i databeskyttelsesforordningens artikel 32, stk. 1.

1. Afgørelse

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

Samtidig finder Datatilsynet, at der er grundlag for at meddele Familieretshuset **påbud** om, at foretage en fornyet risikovurdering, på baggrund af de i denne afgørelse omhandlede brud, herudover skal der på baggrund af risikovurderingen, etableres fornødne organisatoriske eller

[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).

tekniske foranstaltninger. Såfremt Familieretshuset vurderer, at risikoen for de registreredes rettigheder og frihedsrettigheder er høj, indeholder påbuddet også, at Familieretshuset skal udfærdige en konsekvensanalyse, jf. databeskyttelsesforordningens artikel 35.

Påbuddet meddeles i medfør af databeskyttelsesforordningens artikel 58, stk. 2, litra d.

Fristen for efterlevelse af påbuddet er den 6. januar 2023. Datatilsynet skal anmode om senest samme dato at modtage en bekræftelse på, at påbuddet er efterlevet samt hvilke ændringer, i de tekniske og organisatoriske foranstaltninger, der er blevet iværksat.

Ifølge databeskyttelseslovens[2] § 41, stk. 2, nr. 5, straffes med bøde eller fængsel i op til 6 måneder den, der undlader at efterkomme et påbud meddelt af Datatilsynet i medfør af databeskyttelsesforordningens artikel 58, stk. 2, litra d.

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

2. Sagsfremstilling

De i sagen omhandlende brud vedrører videregivelse af beskyttede adresser, beskyttede navne, telefonnumre, e-mailadresser, oplysninger om, hvor børnene går i skole eller institution, opholdssted for den ene part, herunder navne på krisecentre, fornavn og stillingsbetegnelse på lederen af et krisecenter, by eller kommune, som potentielt kan afsløre partens opholdssted over for den uberettigede modtager.

Oplysningerne er i de fleste tilfælde blevet videregivet til den anden part i sagerne, som personerne har haft navne- og adressebeskyttelse for at undgå skulle få oplysningerne, f.eks. på grund af bekymring for børnebortførsel, vold mv. eller fordi parten ikke ønsker kontakt via mail eller telefonisk med den anden part, der evt. også har et tilhold. I nogle tilfælde har den ene forælder også fået nyt navn, for at skjule sig fra den anden forælder.

Oplysningerne er blevet videregivet i forbindelse med besvarelse af aktindsigtsanmodninger, fremsendelse af afgørelser, orienteringsskrivelser og partshøringer. Videregivelserne skyldes hovedsageligt menneskelige fejl i form af, at sagsbehandlerne ikke har været opmærksomme på oplysningerne, og derved ikke har foretaget anonymisering.

Familieretshuset har oplyst til sagen, at Familieretshuset i den konkrete sag vurderer, hvilke foranstaltninger Familieretshuset skal tilbyde den/de registrerede til at afhjælpe uønskede konsekvenser af uberettiget videregivelse af navne- og adresseoplysninger. Sådanne foranstaltninger kan være råd og vejledning om at kontakte politiet hvis nødvendigt, muligheden for at søge erstatning til f.eks. flytteomkostninger eller vejledning til at foretage navneændring.

Som udgangspunkt vil sagsbehandleren forsøge at tage hurtig kontakt til den eller de involverede for at informere om databruddet. Dermed får borgeren de bedste betingelser for at forebygge eventuelle konsekvenser. Sagsbehandleren vil i den forbindelse vejlede om, at borgeren har mulighed for at kontakte Familieretshusets databeskyttelsesrådgiver, hvis borgeren ønsker yderligere vejledning, eller hvis der er behov for særlige foranstaltninger.

I den forbindelse har Familieretshuset oplyst, at i nogle situationer vil sagsbehandleren også tage kontakt til den, der uberettiget har modtaget oplysningerne, hvis dette vurderes hensigts-

[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).

mæssigt. Det kan eksempelvis være tilfældet, hvis modtageren er en kommune, en anden myndighed eller en advokat, der kan forventes at ville medvirke til at slette oplysningerne.

På forældreansvarsområdet, hvor Familieretshuset kan konstatere, at der hyppigst sker databrud, hvor der indgår navne- og adressebeskyttelse, er der ikke et katalog over foranstaltninger. Det vil bero på en konkret vurdering i den pågældende sag og typisk foregå i samarbejde med Familieretshusets databeskyttelsesrådgiver og den centrale juridiske enhed.

Om årsagen til bruddene på persondatasikkerheden, hvor oplysning om beskyttet navn og adresse utilsigtet er blevet videregivet, har Familieretshuset oplyst, at Familieretshuset hvert år behandler tusinde sager. I 2020 traf Familieretshuset afgørelse i 194.976 sager, herunder sager, hvor der indgår beskyttede navne og adresser. Hver sag indeholder ofte en del kommunikationsgange mellem borgerne, andre myndigheder eller læger og Familieretshuset. I den forbindelse har Familieretshuset oplyst, at Familieretshuset derfor har stor fokus på at undgå utilsigtet videregivelse af personoplysninger, og at Familieretshuset kontinuerligt arbejder for at forbedre sikkerheden. Familieretshuset har dog konstateret, at der kan ske menneskelige fejl, når medarbejderne udfører deres arbejde, og at disse fejl desværre kan medføre brud på persondatasikkerheden, hvor beskyttede navne og adresser utilsigtet videregives.

I sager om skilsmisse, hvor der indgår beskyttet navn eller adresse, har Familieretshuset oplyst, at de anvender betegnelserne ”din ægtefælle”, ”mor”, ”far” og ”barn/børn” i stedet for parternes navne.

Familieretshuset har oplyst, at ved aktindsigt og upload til minretssag.dk gennemgås alle dokumenter manuelt, og der er en procedure for, at dokumenterne gennemgås af to medarbejdere for at sikre, at bl.a. beskyttede navne og adresser ikke fremgår af dokumenterne og dermed bliver videregivet utilsigtet.

For så vidt angår sager på forældreansvarsområdet, har Familieretshuset oplyst, at der altid er tale om partstvister. Der er derfor alene en større risiko for databrud, end i sager hvor der kun er én borger eller adressat involveret. Der er som udgangspunkt indlæg fra mindst to parter i hver sag, og parternes indlæg sendes som udgangspunkt i partshøring hos modparten.

Familieretshuset har oplyst, at når parten/parterne har beskyttet navn og adresse, fremgår det altid tydeligt af sagens titel. Derudover beder Familieretshuset parterne oplyse, om Familieretshuset trods navne- og adressebeskyttelse må videregive oplysningerne til den anden part, f.eks. fordi vedkommende allerede er bekendt med oplysningerne.

Hertil har Familieretshuset oplyst, at parterne i myndighedens sager som udgangspunkt har fri adgang til at indsende materiale i det omfang og af den karakter, parten finder relevant og har mulighed for. Sager kan derfor bestå af et bredt sammensat materiale. En anonymisering vil derfor aldrig kunne foregå udelukkende ved en rent teknisk løsning ved brug af f.eks. ’søgerstat’ funktioner eller lignende. Ifølge Familieretshuset vil der derfor altid være en vis risiko for menneskelige fejl.

I enkelte sagstyper bruges der manuel indtastning/indberetninger, hvilket også giver risiko for menneskelige fejl.

På spørgsmålet om, hvad Familieretshuset konkret har gjort for at nedbringe antallet af utilsigtede videregivelser siden Datatilsynets afgørelse over for Familieretshuset af 4. marts 2021, har Familieretshuset oplyst, at de har udpeget 27 GDPR-ambassadører, der skal understøtte arbejdet med databeskyttelse i hele organisationen. Ambassadørerne deltager i netværksmø-

der, hvor databeskyttelse drøftes, og hvor de undervises i de databeskyttelsesretlige regler. Denne viden bringer de med ud til ledelse og kolleger på de kontorer, hvor ambassadørerne er tilknyttet.

GDPR-ambassadørernes synlighed i organisationen betyder, at der er kommet et øget fokus på databeskyttelse.

Familieretshuset har desuden oplyst, at det er et fast punkt på vicedirektør-, kontorchef- og enhedsmøder på driftsområdet at italesætte og gøre opmærksom på forsigtigheden omkring behandling af personoplysninger. Til brug for disse møder udsendes der ca. hver 14. dag ledelsesrapportering ud i forretningen om brud på det respektive vicedirektørområde.

Herudover har Familieretshuset oplyst, at de på familieretsområdet har ændret i deres brevhoveder, således at adressen ikke automatisk bliver indsat. Kun i det omfang borgeren ikke modtager digital post, vil man som sagsbehandler skulle finde adressen og sætte den ind i brevet.

I forhold til sager, der vedrører forældreansvarsområdet, har Familieretshuset oplyst – med henvisning til Datatilsynets afgørelse af 4. marts 2021 – at der er afsat ressourcer til at hjælpe med at anonymisere. Sagsbehandlere på forældreansvarsområdet har mulighed for at bede et team af studentermedhjælpere om at gennemgå sagen og hjælpe med den konkrete anonymisering. På den måde ønsker Familieretshuset at sikre, at der ikke slækkes på proceduren om, at der skal være to sagsbehandlere som gennemgår sagen, på grund af travlhed eller mangel på tidsressourcer.

Videre har Familieretshuset oplyst, at for at sikre opmærksomhed på særlige, konkrete oplysninger af relevans i forhold til databeskyttelse ved en evt. kommende aktindsigt, partshøring eller sagsbehandling i øvrigt, laves der i Familieretshusets sagsbehandlingssystem noter på sagerne. Det sker for at sikre opmærksomhed på beskyttelseshensyn, når en sag skifter sagsbehandler og/eller enhed. Medarbejderne instrueres i forbindelse med onboarding om altid at gennemgå noter på sagsniveau i forbindelse med behandlingen af en sag. Det fremgår bl.a. af visitationskriterierne, hvornår der skal sættes en note på sagen med særlige opmærksomhedspunkter.

Familieretshuset har gjort gældende, at de er opmærksomme på kontinuerligt at forbedre deres sagsgange og vejledning hertil. Det betyder, at hvis Familieretshuset i forbindelse med et konkret databrud opdager eller vurderer, at det konkrete brud kunne være undgået ved en anden procedure, indarbejder Familieretshuset hurtigst muligt læren fra den konkrete fejl i deres generelle arbejdsgange.

Familieretshuset har oplyst, at Familieretshuet generelt indskærper over for sagsbehandlerne, at de skal indarbejde forskellige praktiske rutiner i forbindelse med sagsbehandlingen. Det kan eksempelvis være ikke at have flere sagsvinduer åbent samtidig, når der brevflettes og efterfølgende sendes, og dermed minimere muligheden for en teknisk flettefejl. Det kan også være at indarbejde rutiner med altid at dobbelttjekke og sammenholde navne og adresser på brevene med partsoplysningerne i sagsbehandlingssystemet, inden der sendes.

Det fremgår af Familieretshusets udtalelse, at i konkrete situationer med tekniske udfordringer eller systemfejl er Familieretshuset opmærksom på at informere alle medarbejdere om, hvilke konkrete, midlertidige instrukser de skal følge til afhjælpning af det konkrete problem. Det kan f.eks. være på grund af et udfald på cpr-abonnementet. Der kan i den situation blive givet instruktion om i en periode altid at genfremsøge parterne i F2, inden sagsbehandleren påbe-

gynder eller fortsætter en sagsbehandling, for på den måde at sikre, at parternes oplysninger opdateres med de nyeste oplysninger fra cpr, herunder oplysninger om navne- og adressebeskyttelse.

Hertil har Familieretshuset oplyst, at relevant information bliver kommunikeret via flere kanaler herunder det fælles intranet, konkrete opfølgende mails fra funktionsledere og ved italesættelse på afdelingsmøder og/eller møder i specifikke teams. En konkret ad-hoc instruks vil desuden blive skriftliggjort i Børn og forældreansvars løbende visitationsinstrukser. På den måde sikres det, at forholdsreglerne iagttages på et tidligt tidspunkt i håndteringen af sagerne, og inden sagen overgår til en konkret sagsbehandler.

Familieretshuset har endvidere oplyst, at datasikkerhed indgår som et tema i MUS- og kvartalssamtaler, hvor medarbejderens fokus på datasikkerhed kan drøftes med en funktionsleder. På den måde fastholdes det generelle fokus på datasikkerhed.

Herudover har Familieretshuset oplyst, at datasikkerhed indgår som et væsentligt moment i modtagelse og oplæring af nye medarbejdere. Det gøres ved italesættelse i den konkret afdeling allerede fra starten af ansættelsen. Nye medarbejdere skal derudover tidligt i ansættelsen tage en række kurser og test om data- og it-sikkerhed i Campus og deltage i generelle onboarding-oplæg fra databeskyttelsesrådgiveren og HR. I den forbindelse har Familieretshuset oplyst, at Familieretshuset i det forgangne år og senest i maj 2021 har haft en meget stor udvidelse af medarbejderstaben på forældreansvarsområdet.

Videre har Familieretshuset anført, at på trods af et stærkt fokus på datasikkerhed i både onboarding og konkret oplæring, kan det næppe udelukkes, at den stigning i produktiviteten som den øgede rekruttering har medført, også slår igennem i antallet af databrud. I den sammenhæng har Familieretshuset bemærket, at Familieretshuset siden 1. januar 2020 har øget antallet af årsværk med ca. 380.

Derudover har Familieretshuset oplyst, at direktionen den 9. november 2021 besluttede et koncept for systematisk opfølgning på alle databrud, så fokus øges på at nedbringe antallet af databrud og samtidig sikre, at de rette foranstaltninger iværksættes, så lignende brud ikke sker igen. Konceptet medfører, at alle ledelseslag får kendskab til deres rolle og ansvar i processen, og at håndtering samt mitigerende handlinger overvåges af direktionen. Det vil give Familieretshuset et øget fokus på risici for de registreredes rettigheder og frihedsrettigheder og dermed øget fokus på en risikobaseret tilgang til databeskyttelse i organisationen.

I den forbindelse har Familieretshuset oplyst, at med konceptet bliver det fremadrettet et krav, at GDPR-ambassadører og funktionsledere dokumenterer beslutninger om mitigerende foranstaltninger i forbindelse med hvert brud på persondatasikkerheden. Mitigerende foranstaltninger – og eventuelle beslutninger om, at der ikke skal gennemføres mitigenrende foranstaltninger – skal godkendes af kontorchefer og vicedirektører. Vicedirektører afrapporterer til direktionen, der godkender sektionernes arbejde med databeskyttelse. På baggrund af afrapporteringerne udmelder direktionen overordnede databeskyttelsesretlige emner, som organisationen skal arbejde med. Konceptet vil på sigt blive udvidet til også at omhandle de øvrige krav i databeskyttelsesforordningen samt opgaver inden for informationssikkerhed. Udvidelsen vil ske i takt med, at Familieretshusets re-implementeringsplan gennemføres.

Familieretshuset har desuden oplyst, at Familieretshuset i forbindelse med behandling af adoptions- og værgemålssager overvejer at få systemunderstøttet anonymiseringsopgaven, således at det bliver lettere at fremsøge og skjule oplysninger, der skal anonymiseres.

I forbindelse med sager om separation og skilsmisse er Familieretshuset endvidere ved at undersøge, om det er muligt, at eventuelle børn ikke oprettes som parter på sagen i Familieretshusets sagsbehandlingssystem, for at undgå eventuelt utilsigtet videregivelse ved valg af forkert modtager på sagen.

Afslutningsvist har Familieretshuset oplyst, at generelt forbereder og udfører GDPR-ambassadører i de enkelte afdelinger løbende awareness-begivenheder efter behov og aftale med ledelsen, som en del af deres opgave med at skabe vedvarende opmærksomhed om datasikkerheden. Indsatsen vil fremadrettet blive udbygget yderligere.

3. Begrundelse for Datatilsynets afgørelse

Det følger af databeskyttelsesforordningens artikel 32, stk. 1, at den dataansvarlige 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, skal gennemføre passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til disse risici.

Det følger endvidere af forordningens artikel 32, stk. 1, litra d, at den dataansvarlige, alt efter hvad der er relevant, bl.a. skal gennemføre en procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed.

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 særligt fortrolige og følsomme oplysninger, ikke kommer til uvedkommendes kendskab, **at** der bør udføres passende kvalitetskontrol af indhold i fremsendte dokumenter med henblik på at undgå videregivelser af personoplysninger til uvedkommende, og **at** håndtering af fortrolige og følsomme personoplysninger stiller større krav til medarbejdernes omhyggelighed i forbindelse med fremsendelse af personoplysninger, herunder sikring af at rette oplysninger sendes til rette modtager.

Datatilsynet kan konstatere, at Familieretshuset – efter tilsynets afgørelse af 4. marts 2021 – har gennemført betydelige organisatoriske foranstaltninger for at undgå utilsigtet videregivelse af beskyttede navne- og adresseoplysninger. Det er dog Datatilsynets opfattelse, at nye og gentagne brud på persondatasikkerheden eller hændelser, der skal føres på listen påkrævet efter databeskyttelsesforordningens artikel 33, stk. 5, bør få den dataansvarlige til at reflektere over allerede foretagne risikovurderinger. Brudtyper der henføres til personlige fejl eller enkeltstående episoder – bør ved gentagelse – give anledning til indførelse af yderligere effektive kontrolforanstaltninger eller teknisk understøttelse, der minimerer de nu kendte og aktualiserede risici.

Eksempler på sådanne foranstaltninger kan være, oplysningsminimering sådan at adressen alene bliver benyttet i situationer, hvor den er påkrævet for afgørelsen eller nødvendig for forsendelse med fysisk post, blokering i ESDH-systemet af afsendelse af oplysninger om adresser, andet end til den person hvis adresse det er, eller det kan være indførelse af et egentligt Data Leak Prevention (DLP) system.

Datatilsynet finder, at Familieretshuset – ved at have konstateret og anmeldt flere ligeartede brud på persondatasikkerheden, uden at have genovervejet de eksisterende foranstaltninger med henblik på, at forhindre fremtidige brud af samme type – ikke har truffet passende organisatoriske og tekniske foranstaltninger for at sikre et sikkerhedsniveau, der passer til de risici, der er ved Familieretshusets behandling af personoplysninger, jf. databeskyttelsesforordningens artikel 32, stk. 1. Datatilsynet har særligt lagt vægt på, at Familieretshuset ikke i tilstrækkeligt omfang har haft de fornødne procedurer for regelmæssig efterprøvning, vurdering og evaluering af effektiviteten af de allerede etablerede foranstaltninger.

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

Datatilsynet har ved valg af reaktion i skærpende retning lagt vægt på, at det kan være forbundet med store konsekvenser for de registrerede, når deres beskyttet adresse eller andet opholdssted, som f.eks. navnet på et krisecenter, utilsigtet bliver videregivet til den person, de prøver at skjule sig for.

Samtidig finder Datatilsynet, at der er grundlag for at meddele Familieretshuset **påbud** om, at foretage en fornyet risikovurdering, på baggrund af de i denne afgørelse omhandlede brud, herudover skal der på baggrund af risikovurderingen, etableres fornødne organisatoriske eller tekniske foranstaltninger. Såfremt Familieretshuset vurderer, at risikoen for de registreredes rettigheder og frihedsrettigheder er høj, indeholder påbuddet også, at Familieretshuset skal udfærdige en konsekvensanalyse, jf. databeskyttelsesforordningens artikel 35.

Påbuddet meddeles i medfør af databeskyttelsesforordningens artikel 58, stk. 2, litra d.

Fristen for efterlevelse af påbuddet er den 6. januar 2023. Datatilsynet skal anmode om senest samme dato at modtage en bekræftelse på, at påbuddet er efterlevet samt hvilke ændringer, i de tekniske og organisatoriske foranstaltninger, der er blevet iværksat.

Ifølge databeskyttelseslovens[3] § 41, stk. 2, nr. 5, straffes med bøde eller fængsel i op til 6 måneder den, der undlader at efterkomme et påbud meddelt af Datatilsynet i medfør af databeskyttelsesforordningens artikel 58, stk. 2, litra d.

4. Afsluttende bemærkninger

Datatilsynets afgørelser kan ikke indbringes for anden administrativ myndighed, jf. databeskyttelseslovens § 30. Tilsynets afgørelser kan dog indbringes for domstolene, jf. grundlovens § 63.

[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 afventer herefter en bekræftelse fra Familieretshuset på, at påbuddet er efterlevet.

Datatilsynet forventer at offentliggøre denne afgørelse på tilsynets hjemmeside.

Med venlig hilsen

Betty Husted

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
8) »databehandler«: en fysisk eller juridisk person, en offentlig myndighed, en institution eller et andet organ, der behandler personoplysninger på den dataansvarliges vegne

[…]

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 58, stk. 2. Hver tilsynsmyndighed har alle af følgende korrigerende beføjelser:

[…]

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 […]

Uddrag af 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)

§ 41. Medmindre højere straf er forskyldt efter den øvrige lovgivning, straffes med bøde eller fængsel indtil 6 måneder den, der overtræder bestemmelserne om […]

Stk. 2. På samme måde straffes den, der

[…]

4) undlader at efterkomme et påbud eller en midlertidig eller definitiv begrænsning af behandling eller tilsynsmyndighedens suspension af overførsel af oplysninger i henhold til databeskyttelsesforordningens artikel 58, stk. 2,
5) undlader at efterkomme et påbud fra tilsynsmyndigheden som omhandlet i databeskyttelsesforordningens artikel 58, stk. 2,

[…]