DATATILSYNET

Familieretshuset
Storetorv 10
6200 Aabenraa
Danmark

Sendt med Digital Post

4. marts 2021

J.nr. 2020-432-0037
Dok.nr. 307948
Sagsbehandler
Poul Erik Weidick

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

CVR 11883729

Anmeldelser om brud på persondatasikkerheden

Datatilsynet har gennemgået anmeldelser fra Familieretshuset

Datatilsynet er den centrale, uafhængige myndighed, der fører tilsyn med enhver behandling af personoplysninger, der er omfattet af databeskyttelsesforordningen og databeskyttelsesloven.

Efter en gennemgang af tilsynets sager vedrørende anmeldelser om brud på persondatasikkerheden konstaterede Datatilsynet, at Familieretshuset frem til den 27. september 2020 har anmeldt 158 brud på persondatasikkerheden til tilsynet i overensstemmelse med databeskyttelsesforordningens artikel 33.

Datatilsynet har gennemgået de pågældende anmeldelser for at se, om der er sammenfald i årsagerne til anmeldelserne, og i givet fald hvordan sager af lignende karakter fremadrettet kan undgås. Datatilsynet har derfor indledt en sag af egen drift mod Familieretshuset.

På baggrund af en nærmere gennemgang af de modtagne anmeldelser om brud på persondatasikkerheden, var det Datatilsynets vurdering, at 130 ud af 158 anmeldelser vedrørte utilsigtet videregivelse af personoplysninger.

Datatilsynet skal indledningsvis oplyse, at persondataloven[1] pr. 25. maj 2018 er blevet ophævet og erstattet af databeskyttelsesforordningen[2] og databeskyttelsesloven[3]. Denne afgørelse er derfor truffet efter de nu gældende regler.

Da bruddene på persondatasikkerheden har omfattet perioder, også før databeskyttelsesforordningen fandt anvendelse, har Datatilsynet ladet dette indgå ved fastsættelsen af sanktionen.

Datatilsynet skal videre bemærke, at Familieretshuset organisatorisk bygger på det tidligere "Statsforvaltningen" og før dette "Statsforvaltningerne" og Familieretshuset har således ved ændringen i april 2019 overtaget en lang række af de allerede implementerede it-systemer.

[1] LOV nr. 429 af 31/05/2000 om behandling af personoplysninger, som senest ændret ved lov nr. 410 af 27. april 2017.
[2] 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] 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).

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 artikel 32, stk. 1.

Endvidere finder Datatilsynet, at der er grundlag for at udtale **alvorlig kritik** af, at Familieretshuset ikke i overensstemmelse med databeskyttelsesforordningens artikel 28, stk. 3 har iagttaget kravet om skriftlig databehandleraftale med databehandleren CBRAIN A/S og at der til databehandleraftalen med Visma Consulting A/S ikke var udarbejdet en skriftlig databehandlerinstruks.

Samlet set udtaler Datatilsynet **alvorlig kritik** af Familieretshusets overtrædelser af databeskyttelsesforordningen.

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

2. Datatilsynet har anmodet Familieretshuset om en udtalelse

Af de 158 anmeldte behandlede anmeldelser fra Familieretshuset handlede 130 om utilsigtet videregivelse af personoplysninger, hvorfor Datatilsynet besluttede at tage en sag op af egen drift[4], og anmodede i den forbindelse Familieretshuset om en udtalelse i sagen.

2.1. Opgørelse af anmeldelser af brud på persondatasikkerheden

Datatilsynet bad indledningsvis Familieretshuset fremsende en opgørelse over alle brud på persondatasikkerheden vedrørende utilsigtet videregivelse af personoplysninger hos Familieretshuset i perioden fra den 25. maj 2018 til og med den 27. september 2020, indeholdende de elementer, som følger af forordningens artikel 33, stk. 5. Herunder bad Datatilsynet Familieretshuset om at oplyse, hvor stor en andel de konstaterede sikkerhedsbrud – hvor personoplysninger utilsigtet er videregivet som følge af menneskelige/manuelle fejl – udgjorde af Familieretshusets samlede udadvendte kommunikation med bl.a. borgere, myndigheder m.v.

2.2. Familieretshusets risiko- og konsekvensanalyse

Datatilsynet anmodede Familieretshuset om – i de sager hvor der sker udadrettet kommunikation med bl.a. borgere, myndigheder m.v., i forbindelse med sagsbehandling – at redgøre for Familieretshusets overvejelser om de sikkerhedsmæssige og databeskyttelsesretlige forhold til risikoen for utilsigtet videregivelse af personoplysninger, der var ved behandlingerne og de konsekvenser, som utilsigtet videregivelse af personoplysninger kunne have for de registrerede, særligt i tilfælde hvor oplysninger om beskyttede navne og adresser blev videregivet til en anden part i et konfliktfyldt forhold.

2.3. Familieretshusets tekniske og organisatoriske foranstaltninger

Familieretshuset blev videre bedt om at oplyse, om der er truffet særlige tekniske og organisatoriske sikkerhedsforanstaltninger, med henblik på at sikre, at oplysninger om beskyttede navne og adresser ikke kommer til uvedkommendes kendskab og at fremsende alle givne instrukser (med dato for udarbejdelse) til Familieretshusets medarbejdere omkring håndtering

[4] nærmere regler om Datatilsynets tilsyn findes i databeskyttelseslovens § 27.

af personoplysninger i forbindelse med fremsendelse af oplysninger til bl.a. borgere, myndigheder m.v.

2.4. Manuel behandling eller menneskelige fejl

Da det har fremgået af Familieretshusets anmeldelser til Datatilsynet, at der i forbindelse med sagsbehandling er sket utilsigtet videregivelse af personoplysninger som følge af manuel behandling/menneskelige fejl, bad Datatilsynet Familieretshuset oplyse hvilke relevante organisatoriske og tekniske sikkerhedsforanstaltninger der var etableret forud for brevdatoen for at sikre, at personoplysninger ikke kommer til uvedkommendes kendskab ved utilsigtet videregivelse og hvilke tekniske og organisatoriske foranstaltninger, som Familieretshuset har gennemført, eller har tænkt sig at gennemføre for fremadrettet at undgå utilsigtede videregivelser.

2.5. Selvbetjeningsløsninger

I forbindelse med gennemgangen af de anmeldte brud vedrørende utilsigtet videregivelse af personoplysninger har Datatilsynet konstateret, at en række sager vedrørte utilsigtede videregivelse af personoplysninger i forbindelse med anvendelsen af en eller flere af Familieretshuset selvbetjeningsløsninger.

Datatilsynet har derfor bedt Familieretshuset om at redegøre for de nærmere omstændigheder, der har ført til videregivelse af personoplysninger – herunder oplysninger om beskyttede navne og adresser – i forbindelse med borgeres anvendelse af 5 selvbetjeningsløsninger, der er udført af databehandlerne Charlie Tango A/S (Herefter Charlie Tango), CBRAIN A/S Herefter CBRAIN) og Ditmer A/S (Herefter Ditmer). Familieretshuset er samtidig blevet bedt om at redegøre for de relevante tekniske og organisatoriske sikkerhedsforanstaltninger, som var truffet af Familieretshuset og de pågældende databehandlere forud for bruddet og hvilke, der er gennemført for at håndtere bruddet og med henblik på at standse bruddet.

Datatilsynet har videre anmodet Familieretshuset om at redegøre for om de enkelte databehandlere efter Familieretshusets opfattelse har overtrådt de indgåede databehandleraftaler og instrukser og om at fremsende de relevante databehandleraftaler.

2.6. Familieretshusets regningslinjer for anonymisering

I forbindelse med gennemgangen af et anmeldt brud på persondatasikkerheden, konstaterede Datatilsynet at Familieretshuset har vedhæftet et dokument, der ikke var tilstrækkeligt anonymiseret, hvilket Datatilsynet orienterede Familieretshuset om.

Datatilsynet har anmodet Familieretshuset om at beskrive den procedure for anonymisering, som Familieretshuset anvendte frem til Datatilsynet gjorde opmærksom på fejlen, at fremsende eventuelle procedurer for anonymisering der var gældende inden dette og eventuelt efterfølgende rettede procedurer.

3. Familieretshusets oplysninger til sagen

Familieretshuset har den 15. oktober 2020 fremsendt en indledende udtalelse, som den 2. november 2020 blev suppleret med yderligere oplysninger. Endvidere har Familieretshuset den 9. november 2020 fremsendt en udtalelse, relateret til Familieretshusets selvbetjeningsløsninger.

3.1. Opgørelse over brud på persondatasikkerheden

Familieretshuset har i opgørelsen over brud på persondatasikkerheden anført antallet af sager, hvor der er sket utilsigtet videregivelse af personoplysninger til 134. Af disse brud findes 34 tilfælde, der vedrører personer med beskyttede navne og adresser. I langt den overvejende

del er der tale om menneskelige fejl og i 12 tilfælde er årsagen anført som teknisk fejl, hvoraf 6 kan henføres til fejl ved brevfletning.

Der er ud over almindelige personoplysninger som navn og adresse tale om blandt andet cpr-nummer, helbredsoplysninger, etnicitet, væsentlige sociale problemstillinger, økonomiske forhold, religiøs og filosofisk overbevisning og seksuel orientering. I de 34 tilfælde, hvor der har været tale om beskyttede navne og adresser, er oplysningerne i langt de fleste af tilfældene blevet videregivet til en anden part i sagen og i enkelte tilfælde til fagpersoner, så som læger, advokater, kommuner eller private virksomheder.

3.2. Familieretshusets overvejelser om risici

Familieretshuset har i perioden fra maj 2018 til september 2020 behandlet 421.665 afgørelser og behandlet 13.558 aktindsigtsanmodninger, hvorfor de 134 brud på persondatasikkerheden udgør en meget lille del af Familieretshusets samlede udvekslinger af personoplysninger.

Familieretshuset har ikke desto mindre en vigtig opgave i kontinuerligt at have fokus på borgernes datasikkerhed og følger Datatilsynets vejledning for håndtering af brud på persondatasikkerheden. Derfor har Familieretshuset arbejdet med et øget awareness-niveau blandt medarbejdere og ledere og på bedre uddannelse af medarbejdere med fokus på informationssikkerhed og databeskyttelse. Familieretshuset forventer på den baggrund en stigning af anmeldte brud på persondatasikkerheden.

Familieretshuset bygger organisatorisk på det tidligere Statsforvaltningen og arbejdet med implementering, databeskyttelse og informationssikkerhed har historisk ikke været tilstrækkeligt prioriteret, hvilket har efterladt en betydelig organisatorisk og teknisk gæld og en generel lav modenhed inden for de 2 områder.

Familieretshuset påbegyndte i november 2019 udarbejdelsen af risikovurderinger og konsekvensanalyser, der er forankret i risikomatricer med udgangspunkt i COSO-rammeværket. I maj 2020 godkendte direktionen en 2-årig implementeringsplan på databeskyttelses- og informationssikkerhedsområdet. Erkendelsen af det tidligere utilstrækkelige fokus på de to områder har ledt til at direktionen har tilført yderligere ressourcer, herunder en dedikeret projektleder. Familieretshuset har i efteråret 2020 påbegyndt afdækning af behov for yderligere ressourcer til området.

3.3. Familieretshusets overvejelser om konsekvenser

Familieretshuset behandler mange sager, hvor parterne ønsker beskyttet navn og adresse. Familieretshuset har erfaret, at det er af afgørende betydning, at der er en afklaring om hvorvidt navne- og adressebeskyttelsen er gældende. Derfor indleder Familieretshusets sagsbehandling altid med en afklaring af hvorvidt sagen er beskyttet og hvorvidt denne beskyttelse er gældende over for sagens øvrige parter. I de tilfælde, hvor navne- og adressebeskyttelse imellem parterne skal opretholdes, gør Familieretshuset en særlig indsats for at sikre fortroligheden af dette mellem parterne og Familieretshusets medarbejdere er fuldt ud bevidste om de vidtrækkende konsekvenser det kan få for de implicerede, hvis der sker utilsigtet videregivelse af personoplysninger. Disse store konsekvenser er indeholdt i Familieretshusets risikovurderinger og risikovillighed i udviklingen af nye tekniske løsninger og organisatoriske processer og arbejdsgange.

3.4. Særlige foranstaltninger i forbindelse med navne- og adressebeskyttelse

Hos Familieretshuset er der altid 2 sagsbehandlere, der gennemgår materialet inden videregivelse. I de tilfælde, hvor der skal opretholdes navne- og adressebeskyttelse mellem parterne, gør Familieretshuset en særlig indsats for at sikre fortroligheden, bl.a. gennem undta-

gelse og anonymisering. Der er til dette formål i 2020 udarbejdet et notat for anonymisering og pseudonymisering. Alle akter angives med teksten ”Beskyttet navn og adresse*” for at mindske sandsynligheden for at fejlopstår, især ved sagsbehandlerskift.

Et led i uddannelsen af medarbejderne er at sikre en hurtig underretning af de registrerede med henblik på at reducere de negative konsekvenser for de registrerede i tilfælde af brud på persondatasikkerheden.

Familieretshuset har siden 2019 arbejdet på at samle opgaven for oversendelse af sagsakter og personoplysninger til retten til et specialiseret team for at mindske sandsynligheden for fejl.

Som teknisk foranstaltning har Familieretshuset planlagt at udvikle en forsinket afsendelse af dokumenter fra Familieretshusets ESDH-system, der vil medføre, at medarbejdere har mulighed for at trække korrespondance tilbage inden for en forud defineret tidsperiode. Da Familieretshusets IT-drift i slutningen af 2020 skal overgå til Statens IT, forventes denne løsning at kunne være i drift i andet kvartal af 2021.

I samarbejdet med Domstolsstyrelsen er også konstateret en række uretmæssige overførsler til ”min-retsag.dk”. På dette område er udarbejdet en procedure der kan gøre oplysningerne utilgængelige for parterne og samtidig bevisindsamle oplysninger for den uberettigede videregivelse. Det er således muligt at afgøre hvorvidt oplysningerne reelt er tilgået og således reducere de negative konsekvenser for de registreredes rettigheder.

Beskyttelse af navne- og adresseoplysninger har været et særskilt punkt ved udviklingen af nye tekniske løsninger af forretningen, herunder blandt andet krypteret videoløsning, hvortil der også er udarbejdet instrukser til medarbejderne om kontrol af hvorvidt parterne har beskytet navn og adresse.

I forbindelse med de konstaterede sikkerhedsbrud i nogle af Familieretshusets selvbetjeningsløsninger i august 2020, har Familieretshuset gennemgået samtlige borgerrettede selvbetjeningsløsninger med henblik på at sikre, at lignende fejl ikke er tilstede. I de tilfælde er løsningerne blevet lukket og bruddene er anmeldt til Datatilsynet.

Det er Familieretshusets klare hensigt, at selvbetjeningsløsningerne skal indeholde tekniske sikkerhedsforanstaltninger, der sikrer, at der ikke videregives beskyttede navne og adresser til uvedkommende. I den forbindelse har Familieretshuset indgået aftale med en ekstern revisionsvirksomhed om at gennemgå hændelsesforløb og systemer for alle borgerrettede IT-løsninger, samt at bidrage med input til en governance-model, der sikrer en fremtidig effektiv velkoordineret og robust struktur for arbejdet med IT sikkerhed, Informationssikkerhed, ISO modenhed og GDPR. Rapporten er fremsendt til Datatilsynet.

Familieretshuset har videre fremsendt bilag med vejledninger og instruktioner for Familieretshusets medarbejdere omkring håndtering af personoplysninger i forbindelse med fremsendelse af materiale til borgere, myndigheder m.v.

3.5. Foranstaltninger for at imødegå manuelle og menneskelige behandlingsfejl

Familieretshuset har den 5. maj 2020 iværksat en større implementeringsplan, der skitserer en række aktiviteter og fokusområder for den næste 2 år. Der er udpeget en større gruppe decentrale ambassadører, der i løbet af 2021 vil blive uddannet i en lang række centrale databeskyttelsesretlige spørgsmål. Det er også planen at sætte fokus på procedurer og arbejdsgange, gennemgang af databehandleraftaler, udarbejdelse af en ny politik for databeskyttelse efter databeskyttelsesforordningen, samt uddannelse af de decentrale ambassadører.

Desuden sætter Familieretshuset fokus på nye procedurer i porteføljestyring, auditering af leverandører og kontraktopfølgning.

3.6. Familieretshusets selvbetjeningsløsninger

Familieretshuset giver borgere adgang til i alt 40 selvbetjeningsløsninger inden for blandt andet adoption, bidrag, faderskab, forældreansvar, klager, skilsmisse, værgemål og ægteskab for internationale par. For 11 af disse løsninger – henholdsvis samvær, bopæl, konfirmationsbidrag, enighedsansøgning for børnebidrag, registrering af delt bopæl, registrering af ophør af delt bopæl, ansøgning om ændring af forældremyndighed for ikke-biologiske forældre, ændring af bopæl og ansøgning om at blive adoptant – har Familieretshuset modtaget henvendelser om brud på persondatasikkerheden forbundet med uretmæssig videregivelse af navn på borgere med navne- og adressebeskyttelse.

Databruddene er relateret til en teknisk mangel på grund af en kodefejl i et CPR-kald, der anvendes i løsninger, der er udbudt af leverandørerne Charlie Tango og CBRAIN.

3.7. Selvbetjeningsløsning for forældremyndighed, bopæl og samvær

På baggrund af en borgerhenvendelse den 13. august 2020 konstaterede Familieretshuset den 17. august 2020 en fejl i selvbetjeningsløsningen, hvor primært forældre, men også andre ansøgere (eksempelvis bedsteforældre) kan søge om forældremyndighed, bopæl og samvær. Integrationen mellem selvbetjeningsløsningen og navne- og adressebeskyttelsesregistreringen i CPR-registeret fungerede ikke korrekt, hvilket medførte, at der på de automatiske genererede kvitteringer for indleverede ansøgninger fremgik fulde navn på de involverede børn, selvom disse stod registreret med navne- og adressebeskyttelse i CPR-registret.

Løsningen blev leveret af Charlie Tango som er databehandler og underleverandør til Visma Consulting A/S (herefter Visma), med hvem det daværende Statsforvaltningen indgik kontrakt med i 2018. Der foreligger en databehandleraftale med Visma, men ikke en udfyldt databehandlerinstruks.

Indledningsvis meddelte underleverandøren Charlie Tango, at der ikke var et problem i løsningen, men fandt samme dag et væsentligt problem i integrationen til CPR-registret.

3.8. Selvbetjeningsløsning for konfirmations- og beklædningsbidrag

Den daværende Statsforvaltning implementerede i januar 2016 en række borgerrettede selvbetjeningsløsninger, herunder for konfirmations- og beklædningsbidrag. Forvaltningen var forinden implementeringen opmærksom på at systemet ikke i CPR-kaldet kunne adskille typen af kvitteringssvar, hvorfor der var risiko for, at persondata for personer med navne- og adressebeskyttelse kunne blive videregivet uretmæssigt. Der blev derfor anført en meddelelse i selvbetjeningsløsningen hvoraf det fremgik, at personfølsomme data ville blive videregivet til begge barnets forældre, uanset en eventuel navnebeskyttelse. Ønskedes dette ikke, blev borger henvist til at anvende en alternativ manuel blanket.

Familieretshuset konstaterede d. 19. august 2020 et brud på persondatasikkerheden i Familieretshusets selvbetjeningsløsning, hvor forældre kan søge om konfirmations- og beklædningsbidrag ved den anden forælder. Det blev konstateret, at Familieretshuset uberettiget havde videregivet oplysninger om beskyttet navn på barnet og den ansøgende forælder til den anden forælder.

Den 15. april 2020 oprettede Familieretshuset en ændringsanmodning hos CBRAIN til udbedring af fejlen, men dette blev ikke i gangsat på grund af "frozen period" op mod ovegang til Statens IT.

3.9. Selvbetjeningsløsning ved brug af DitmerFlex-løsninger

Der blev den 17. december 2017 indgået databehandleraftale mellem den daværende Statsforvaltning og Ditmer om intern udvikling DitmerFlex selvbetjeningsløsninger med anvendelse af Nem-ID login og digital post. Systemerne blev testet internt og sat i drift med en efterfølgende hypercare periode. Den 7. september 2020 blev Familieretshuset bekendt med, at 4 af løsningerne – enighedsansøgning ang. bidrag, registrering af delt bopæl samt registrering af ophør af delt bopæl og ansøgning om at blive adoptant – videregav beskyttede navne på borgere, ved, at den anden part i sagen fik tilsendt en kopi partens ansøgning/registrering, hvori der ikke blev taget højde for evt. beskyttet navn på parten og det i ansøgningen/registreringen omhandlede barn. Løsningerne blev herefter lukket.

Det blev besluttet, at løsningerne først ville blive taget i brug når systemerne blev forhindret i at videregive beskyttede navn uden samtykke og der forelå løsning til gyldigt samtykke.

Det er Familieretshusets opfattelse, at der ikke er tale om en kompromittering af Ditmers løsning, men at fejlen er opstået i forbindelse med den måde Familieretshusets har anvendt DitmerFlex.

3.10. Henvendelser om berørte selvbetjeningsløsninger

Familieretshuset har den 20. november 2020 oplyst, at for i alt 11 selvbetjeningsløsninger har Familieretshuset modtaget henvendelser om uberettiget videregivelse af navn på borgere med navne- og adressebeskyttelse som følge af fejlen i CPR-kaldet.

3.11. Underretning til de registrerede

Familieretshuset har vurderet, at i alt 3493 borgeres personoplysninger muligvis er blevet uretmæssigt videregivet og disse personer er, med bistand af CPR-kontoret, blevet underrettet.

Familieretshuset udsendte på den baggrund fredag d. 28.08.2020 underretning om bruddene på persondatasikkerheden til i alt ca. 3400 registrerede, som var tilmeldt digital post.

Underretningerne fordeler sig på ca. 1.300 til forældre, som var omfattet af databruddet på konfirmationsbidragsløsningen, ca. 160 til unge over 18 år, som var omfattet af databruddet på konfirmationsbidragsløsningen, ca. 1.800 til forældre, som var omfattet af databruddet på forældremyndighed, bopæl og samværsløsningen og ca. 210 til unge over 18 år, som var omfattet af databruddet på forældremyndighed, bopæl og samværsløsningen.

Derudover har Familieretshuset fremsendt 76 underretninger med fysisk post (som Quickbrev), da modtagerne ikke var tilmeldt/fritaget for digital post. Endelig er 276 tilfælde udtaget til manuel behandling, da det ud fra det foreliggende datagrundlag ikke var entydigt, i hvilket omfang og til hvem der skulle ske underretning. Dette har resulteret i afsendelse af yderligere ca. 100 underretningsbreve med digital post.

Familieretshuset identificeret de direkte berørte registrerede samt underrettet dem, som vurderedes at være i risikogruppen. Ved vurderingen har Familieretshuset lagt til grund, at modtageren af oplysningen om det beskyttede navn – i de fleste tilfælde den anden forælder – oftest vil have kendskab til navnet på sine børn og sin tidligere partner i forvejen. I de tilfælde hvor der ikke i forbindelse med registreringen af navnebeskyttelsen ligeledes er foretaget tiltag til ændring af navn som led i identitetsbeskyttelse, er det Familieretshusets vurdering, at

videregivelsen af et beskyttet navn ikke har bibragt den anden forælder/ansøgeren oplysninger, som denne ikke allerede var bekendt med.

Konkret har Familieretshuset foretaget en manuel gennemgang af alle de tilfælde, hvor der ud over navnebeskyttelse også er foretaget navneændring. Herefter har Familieretshuset foretaget en individuel vurdering af, hvorvidt de pågældende registrerede vurderes at kunne være direkte berørte af databruddet pga. forsøg på identitetsbeskyttelse.

På baggrund heraf har Familieretshusets estimeret, at der kan være 11 direkte berørte, som i forbindelse med anvendelse af selvbetjeningsløsningen for ansøgning om forældremyndighed, bopæl og samvær har fået videregivet det beskyttede navn på deres barn, og at der kan være 5 direkte berørte, som i forbindelse med anvendelse af selvbetjeningsløsningen for ansøgning om konfirmations-/beklædningsbidrag har fået videregivet deres eller deres barns beskyttede navn.

I det omfang disse 16 personer ikke allerede har været i kontakt med Familieretshuset gennem vores hotline eller vores databeskyttelsesrådgiver, har Familieretshuset forsøgt at kontakte dem direkte telefonisk med henblik på at give råd og vejledning. Disse direkte berørte har dog under alle omstændigheder modtaget et underretningsbrev.

3.12. Databehandleraftaler og databehandlerinstrukser
Familieretshuset har ikke indgået databehandleraftale med CBRAIN.

Familieretshuset har fremsendt kontrakt, der er indgået med Visma for så vidt angår underleverandøren Charlie Tango. Charlie Tango har udført ydelser i henhold til kontrakt med Visma, men der foreligger ikke formaliseret og udfyldt databehandlerinstruks, hvorfor den ikke opfylder betingelserne i henhold til databeskyttelsesforordningens artikel 28, stk. 3. Der er efter Familieretshusets opfattelse ikke tale om en overtrædelse af indgåede instrukser men en fejl i opsætning af testmiljøet.

Familieretshuset har videre fremsendt databehandleraftale med Ditmer. Aftalen ses dog ikke underskrevet af Ditmer. Det er ikke Familieretshusets opfattelse at databehandleraftalen er overtrådt, da der ikke er tale om kompromittering af Ditmers løsning. Fejlen beror på den måde Familieretshuset har anvendt løsningen.

3.13. Implementering af gyldigt samtykke
Da den praksis omkring beskyttede navne og adresser, som den daværende Statsforvaltning havde anvendt siden 2016 blev betragtet som værende i strid med god praksis og gældende lovgivning, blev der den 15. april 2020 oprettet en ændringsanmodning hos CBRAIN til udbedring af problematikken i forbindelse med CPR-kald, men dette blev ikke igangsat på grund af ”frozen period” op mod ovegang til Statens IT.

I forbindelse med Familieretshusets egenudvikling af blanketløsninger i programmet Ditmer-Flex, har Familieretshuset udarbejdet og implementeret et gyldigt samtykke for 3 af disse selvbetjeningsløsninger. Selvbetjeningsløsningerne fungerer således, at såfremt ansøger/part oplyser, at denne har beskyttet navn i CPR, og at dette ikke må videregives, så henvises der til at ansøge/registrere det aktuelle ærinde ved udfyldelse af en PDF-blanket, som herefter indsendes til Familieretshuset. Ansøgningen/registreringen bliver herefter behandlet manuelt af Familieretshuset. Familieretshuset har oplyst, at samtykket ligeledes vil blive implementeret i Familieretshuset PDF-blanketter for de nævnte løsninger. Dette arbejde pågår.

3.14. Familieretshusets procedure for anonymisering

Familieretshuset har på Datatilsynets anmodning fremsendt procedure for anonymisering og pseudonymisering, dateret den 2. marts 2020. Proceduren er ikke ændret efterfølgende.

Af et anmeldt brud på persondatasikkerheden, Datatilsynets j.nr. 2020-442-8139, fremgår, at der den 13. maj 2020 skete en tilsigtet videregivelse af personoplysninger, idet der blev fremsendt et utilstrækkeligt anonymiseret dokument til en fagforening i stedet for et hospital. Familieretshuset har oplyst, at der var tale om en menneskelig fejl.

4. Deloittes rapport

Konsulentfirmaet Deloittes har på Familieretshusets foranledning den 18. november 2020 udfærdiget en rapport om forretningsgange og teknikske aktiviteter i forbindelse med selvbetjeningsløsningernes CPR-kald. Rapportens indhold er i al væsentlighed i overensstemmelse med Familieretshusets redegørelse. I rapporten har Deloitte anført, at:

> *De to rapporterede databrud vedrører systematisk eksponering af navne på børn og forældre over for den anden forælderpart på trods af disse personers tilvalg af og mulige behov for navne- og adressebeskyttelse over for den anden forælder. Selvbetjeningsløsningerne er borgerrettede, og eksponeringen har været indlejret i løsningernes automatik, hvorfor bruddene vurderes af Familieretshusets Data Protection Officer (DPO) som værende af høj risiko, idet eksponeringens omfang og konsekvenser kan have været vidtrækkende.*

Deloitte har videre i forbindelse med undersøgelsen anført, at Familieretshuset og CBRAIN i implementeringsfasen og ved senere opdateringer af selvbetjeningsløsningen for konfirmationsbidrag ikke har haft en testfrekvens i systemet, men at test er udført ad hoc. Testmetoden har efterladt en væsentlig risiko for menneskelige fejl i testudførelsen, som ikke ville være til stede ved eksempelvis automatiserede test. Deloitte har endvidere konstateret, at der ikke blev foretaget test af ændringernes effekter i produktionsmiljøet, men at der i stedet har været anvendt en såkaldt ”hyper-care-periode”, der dog ikke har været formaliseret i form af klare definitioner på, hvilke overvågningsaktiviteter der skal udføres og frekvensen heraf.

På baggrund af undersøgelserne konstaterede Deloitte, for så vidt angik løsningen for ansøgning om samvær, at data i testmiljøet ikke har haft tilstrækkelig lighed med produktionsmiljøet, hvorfor testene ikke har været effektive i afdækningen af risici for eksponering af beskyttede data i forbindelse med løsningens CPR-kald. Deloitte konkluderede videre, at et andet indrapporteret brud på persondatasikkerheden i samværsløsningen – i form af at beskyttede navne har været synlige i samværsløsningen – relaterede sig til en lignende teknisk afvigelse i CPR-kaldet. Den tekniske afvigelse i CPR-kaldet har eksisteret i løsningen siden implementeringen i april 2019.

Deloittes har på baggrund af undersøgelsen konkluderet, at:

> *På baggrund af undersøgelsen står det klart, at alle de identificerede databrud i forbindelse med CPR-kald har eksisteret i løsningerne siden deres implementering. For konfirmationsbidrag og forældreansvar skete implementeringen hhv. den 26. januar 2016 og 1. april 2019. Manglen er dokumenteret til at have en teknisk karakter, idet løsningernes kodning ikke lykkedes med at adskille hhv. datavisning og kvitteringsvar, afhængigt af om de relaterede borgere havde navnebeskyttelse eller ej, hvorfor beskyttede, personfølsomme data er blevet uretmæssigt videregivet gennem forældreansvarsløsningernes trin 4 og processen for automatisk kvitteringsskrivelse i alle fire løsninger.*

Det står klart i undersøgelsen, at Familieretshusets organisation historisk har været vidende om fejlen og konsekvenserne heraf for konfirmationsbidragsløsningen, hvilket dog ikke er tilfældet med forældreansvarsløsningerne. Opmærksomheden i organisationen har været bragt op i forskellige fora internt ad flere omgange, primært ved løsningens implementering, hvor et notat om problemet blev udarbejdet, men også så sent som i foråret 2020, hvor flere funktionsledere og den ansvarlige vicedirektør blev gjort opmærksom på risikoen for brud, dog uden at dette førte til effektiv afhjælpning. Organisationen har generelt taget mange gode opmærksomhedsinitiativer på området for informationssikkerhed, men det er konstateret, at en manglende forankring i risikovurderinger, politikker og procedurer har været medvirkende til, at organisationen og ledelsen ikke effektivt har fået kommunikeret og afhjulpet bruddene tidligere.

Deloitte har på baggrund af rapportens observationer anbefalet, at Familieretshuset prioriterer en række aktiviteter til udbedring af de observerede risici og implementering af styrkede rammer for organisationens fremtidige arbejde på området for datahåndtering og informationssikkerhed.

5. Begrundelse for Datatilsynets afgørelse

Datatilsynet har ved en gennemgang af Familieretshusets fremsendte redegørelse og tilhørende bilag, samt Deloittes omfattende gennemgang af Familieretshusets forretningsgange og tekniske aktiviteter i forbindelse med sikkerhedsbrud i 2 selvbetjeningsløsninger, fået indblik i en række af Familieretshusets behandlinger. Dette omfatter retningslinjer for udvikling, risikovurderinger, kontrol med databehandleraftaler, de tekniske løsningers modenhed, drifts- og testmiljøer, medarbejdernes omhu ved sagsbehandlingen, de etablerede tekniske og organisatoriske foranstaltninger for at sikre et passende sikkerhedsniveau, samt familieretshusets ledelses viden om disse forhold.

Familieretshuset har i sin redegørelse anført, at Familieretshuset organisatorisk bygger på det tidligere ”Statsforvaltningen” og før dette ”Statsforvaltningerne” og Familieretshuset har således ved ændringen i april 2019 har overtaget en lang række af de allerede implementerede itsystemer. Familieretshuset har i redegørelsen vedstået, at arbejdet med implementering af databeskyttelse og informationssikkerhed historisk set ikke har været et tilstrækkeligt prioriteret område, hvilket har efterladt en betydelig organisatorisk og teknisk gæld, samt en generel lav modenhed inden for de to områder.

Datatilsynet lægger ud fra Familieretshusets egne oplysninger og den af Deloitte foretagende undersøgelse til grund, at en række selvbetjeningsløsninger i flere år – for selvbetjeningsløsningen for konfirmationsbidrag helt tilbage fra 2016 – har anvendt fejlbehæftede CPR-kald, hvilket har betydet, at løsningerne ikke har kunnet afgøre hvorvidt en borger, der anvendte løsningerne, havde beskyttet navn og adresse, hvorfor borgerens personoplysninger uberettiget kunne blive videregivet til uvedkommende i forbindelse med fremsendelse af dokumenter relateret til borgerens sag.

Endvidere lægger Datatilsynet til grund, at Familieretshuset har kendt til det fejlbehæftede CPR-kald, idet der i løsningen i 2016 blev indført en besked til brugere af løsningen, at vedkommendes navn ville blive videregivet til andre, uanset en eventuel navnebeskyttelse.

På baggrund af Deloittes redegørelse, lægger Datatilsynet endvidere til grund, at der ved udviklingen af systemerne ikke er blevet foretaget tilstrækkelig afprøvning af de pågældende systemer, blandt andet fordi testmiljø og produktionsmiljø ikke var ens og der ikke var udarbejdet klare retningslinjer for test og dokumentation af systemerne, herunder for kritiske systemer som CPR-kald.

Som følge af Familieretshusets 134 anmeldelser om utilsigtet videregivelse af personoplysninger, heraf i 34 tilfælde oplysninger om personers med navne- og adressebeskyttelse, er det Datatilsynets opfattelse, at Familieretshuset – som følge af menneskelige fejl, der kan henføres til medarbejdere – ikke har truffet passende og tilstrækkelige tekniske og organisatoriske foranstaltninger til at sikre vedvarende fortrolighed for disse oplysninger.

Med baggrund i Familieretshusets opgaver, lægger Datatilsynet videre til grund, at Familieretshuset behandler mange meget følsomme og fortrolige oplysninger om en stor del af befolkningen og at fremsendelse af disse oplysninger til forkerte modtagere, kan have alvorlig indvirkning på den enkelte borgers rettigheder og i yderste tilfælde sikkerhed, liv og helbred.

5.1. 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 fremgår 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 til at sikre et sikkerhedsniveau, der passer til 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 følsomme oplysninger, ikke kommer til uvedkommendes kendskab, **at** alle sandsynlige fejlscenarier bør testes i forbindelse med udviklingen af ny software, hvor der behandles personoplysninger, **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 følsomme personoplysninger stiller større krav til medarbejdernes omhyggelighed i forbindelse med fremsendelse af personoplysninger, herunder sikring af at rette oplysninger sendes til rette modtager.

Det er videre Datatilsynets opfattelse, at Familieretshusets risikovurderinger ikke i tilstrækkelig grad adresserer risikoen for og konsekvensen ved, at medarbejdere ved fejl, misforståelser eller uopmærksomhed sender oplysninger om registrerede til uvedkommende modtagere, hvilket kan have alvorlige konsekvenser for de registrerede.

5.2. Tekniske foranstaltninger test

Datatilsynet finder, at Familieretshuset, ved ikke at udføre tilstrækkelig og regelmæssig afprøvning af de udviklede selvbetjeningsløsninger, inden de blev sat i drift og ved ikke at sikre, at de anvendte testmiljøer var af en karakter, der gjorde dem egnede til at udføre denne afprøvning, ikke har opfyldt databeskyttelsesforordningens artikel 32, stk. 3, litra d.

Det er Datatilsynets opfattelse, at testmiljøer – sammenholdt med teststrategier og klare retningslinjer – skal have en sådan karakter, at de giver et retvisende billede af hvordan de te-

stede systemer vil agere i produktionsmiljøet og at afprøvningen regelmæssigt skal vurderes og evalueres, således at fejl kan afdækkes inden systemerne bliver sat i produktion.

Det er videre Datatilsynets opfattelse, at løsninger, der indeholder oplysninger af den karakter Familieretshuset behandler, ikke bør være designet til som udgangspunkt at eksponere data, men i stedet være designet til som udgangspunkt at beskytte personoplysningerne og kun eksponere dem, når det er relevant.

Det er Datatilsynets opfattelse, at en registreret ikke ved samtykke kan give afkald på den beskyttelse af sine rettigheder som f.eks. databeskyttelsesforordningens artikel 32, er udtryk for. I de selvbetjeningsløsninger, hvor Familieretshuset har implementeret det Familieretshuset kalder et gyldigt samtykke – og hvor de henviser borgere, der har beskyttet navn og adresse, til at udfylde en blanket og sende denne til Familieretshuset i stedet for at anvende selvbetjeningsløsningen – finder Datatilsynet det herudover tvivlsomt om en sådan information skulle kunne indgå i et samtykke, der ville leve op til definitionen i databeskyttelsesforordningens artikel 7.

5.3. Organisatoriske foranstaltninger

Datatilsynet finder videre, at Familieretshuset, ikke i tilstrækkelig grad har sikret, at medarbejderne har haft den fornødne omhu ved behandling af borgernes personoplysninger, herunder beskyttede navne- og adresseoplysninger. Derved har Familieretshuset ikke levet op til databeskyttelsesforordningens artikel 32, stk. 1, litra b.

Det er Datatilsynets vurdering, at de menneskelige fejl kunne være undgået under iagttagelse af fornøden omhu fra medarbejdernes side, ligesom den ekstra kontrol, der bliver udført af en anden sagsbehandler, åbenbart ikke er tilstrækkelig effektiv. Samtidig bør Familieretshuset indføre effektive tekniske kontrolforanstaltninger ved fremsendelse af sagsbehandlingsdokumenter via elektronisk post, således at disse dokumenter ikke ved en fejl sendes til uvedkommende.

Datatilsynet finder på ovenstående baggrund, 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.

5.4. Databehandleraftaler

Datatilsynet lægger – ud fra Familieretshusets egen forklaring og fremsendte bilag – til grund, at Familieretshuset ikke har indgået kontrakt med CBRAIN og at den indgåede kontrakt med Visma ikke opfylder de formelle betingelser for databehandleraftaler jf. databeskyttelsesforordningens artikel 28, stk. 3

Datatilsynet finder på denne baggrund, 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 28, stk. 3.

Det er Datatilsynets opfattelse, at en kontrakt mellem den dataansvarlige og dennes databehandler skal indeholde alle de elementer der er nødvendige for at fastsatte genstanden for og varigheden af behandlingen, behandlingens karakter og formål, typen af personoplysninger og kategorierne af registrerede, databehandlerens forpligtelser, samt den dataansvarliges ansvar og forpligtelser i overensstemmelse med reglerne i databeskyttelsesforordningens artikel 28, stk. 3.

5.5. Valg af sanktion

Datatilsynet har ved valg af reaktion lagt vægt på, at Familieretshuset behandler mange meget følsomme og fortrolige oplysninger om en stor del af befolkningen og at videregivelse af disse oplysninger, kan have alvorlig indvirkning på den enkelte borgers rettigheder og i yderste tilfælde sikkerhed, liv og helbred.

Samtidig har Datatilsynet lagt vægt på, at overtrædelserne – efter det oplyste – har stået på siden 2016 og at overtrædelserne har været kendt blandt organisationens medarbejdere og mellemledere i flere år. I april 2020 blev funktionsledere og den ansvarlige vicedirektør orienteret om problemstillingen, men planlagte mitigerende foranstaltninger blev prioriteret lavt og kom derfor ikke i gang. Datatilsynet har videre lagt vægt på det høje antal af personoplysninger, der behandles, ligesom oplysningerne vedrører personer, hvoraf mange bør nyde særlig beskyttelse.

Herudover har Datatilsynet lagt vægt på at Familieretshuset har overtaget den tidligere Statsforvaltnings opgaver og dermed en betydelig organisatorisk og teknisk gæld, samt en generel lav modenhed inden for de to områder, forhold som Familieretshuset arbejder målrettet på at rette op på. Datatilsynet har også lagt vægt på, at Familieretshuset i 2020 har iværksat en større implementeringsplan med henblik på at imødegå manuelle og menneskelige behandlingsfejl.

5.6. Databeskyttelsesforordningens artikel 34

Det følger af forordningens artikel 34, stk. 1, at når et brud på persondatasikkerheden sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder, underretter den dataansvarlige uden unødig forsinkelse den registrerede om bruddet på persondatasikkerheden.

Datatilsynet finder, at Familieretshuset har handlet i overensstemmelse med databeskyttelsesforordningens artikel 34, stk. 1.

Datatilsynet har i den forbindelse lagt vægt på, at Familieretshuset i samarbejde med databehandlerne og CPR-registret har foretaget en nøje gennemgang af alle de personer, der blev berørt af bruddene og efter konkret vurdering har underrettet de berørte om hændelserne.

5.7. Sammenfatning

På ovenstående baggrund 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.

Endvidere finder Datatilsynet, at der er grundlag for at udtale **alvorlig kritik** af, at Familieretshuset ikke i overensstemmelse med databeskyttelsesforordningens artikel 28, stk. 3 har iagttaget kravet om skriftlig databehandleraftale med databehandleren CBRAIN og at der til databehandleraftalen med Visma ikke var udarbejdet en skriftlig databehandlerinstruks.

Samlet set giver gennemgangen anledning til, at Datatilsynet udtaler **alvorlig kritik** af Familieretshusets overtrædelser af databeskyttelsesforordningen.

6. Afsluttende bemærkninger

Datatilsynet vil løbende foretage kontrol af Familieretshusets behandling af personoplysninger, særligt med fokus på utilsigtet videregivelse af oplysninger om personer med navne- og adressebeskyttelse.

Det skal for god ordens skyld oplyses, at Datatilsynet forventer at offentliggøre denne afgørelse.

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 34. Når et brud på persondatasikkerheden sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder, underretter den dataansvarlige uden unødig forsinkelse den registrerede om bruddet på persondatasikkerheden.

Stk. 2. Underretningen af den registrerede i henhold til denne artikels stk. 1 skal i et klart og forståeligt sprog beskrive karakteren af bruddet på persondatasikkerheden og mindst indeholde de oplysninger og foranstaltninger, der er omhandlet i artikel 33, stk. 3, litra b), c) og d).

Stk. 3. Det er ikke nødvendigt at underrette den registrerede som omhandlet i stk. 1, hvis en af følgende betingelser er opfyldt:

a) den dataansvarlige har gennemført passende tekniske og organisatoriske beskyttelsesforanstaltninger, og disse foranstaltninger er blevet anvendt på de personoplysninger, som er berørt af bruddet på persondatasikkerheden, navnlig foranstaltninger, der gør personoplysningerne uforståelige for enhver, der ikke har autoriseret adgang hertil, som f.eks. kryptering
b) den dataansvarlige har truffet efterfølgende foranstaltninger, der sikrer, at den høje risiko for de registreredes rettigheder og frihedsrettigheder som omhandlet i stk. 1 sandsynligvis ikke længere er reel
c) det vil kræve en uforholdsmæssig indsats. I et sådant tilfælde skal der i stedet foretages en offentlig meddelelse eller tilsvarende foranstaltning, hvorved de registrerede underrettes på en tilsvarende effektiv måde.

Stk. 4. Hvis den dataansvarlige ikke allerede har underrettet den registrerede om bruddet på persondatasikkerheden, kan tilsynsmyndigheden efter at have overvejet sandsynligheden for, at bruddet på persondatasikkerheden indebærer en høj risiko, kræve, at den dataansvarlige gør dette, eller beslutte, at en af betingelserne i stk. 3 er opfyldt.