DANMARKS FONDE

Rapport: Mange fonde sjusker med personoplysninger

Langt de fleste fonde håndterer ansøgninger via e-mail, viser en ny markedsundersøgelse foretaget af firmaet Exformatics. Men fondenes udbredte brug af e-mail kan let bringe fondene på kant med persondatareglerne. Sådan lyder advarslen fra flere eksperter, der bekræfter undersøgelsens budskab om, at mange fondene endnu ikke er i mål med GDPR.

af Sune Holm Pedersen – 20. august 2019

Fondene er endnu ikke i mål med GDPR. Sådan lyder den overordnede konklusion i en ny rapport udarbejdet for firmaet Exformatics, der sælger digitale administrationsløsninger til fonde.

Rapporten 'Danske Fondes Digitaliseringsniveau' er baseret på interviews med 87 forskellige fonde om blandt andet deres behandling af persondata. Og ifølge flere eksperter giver fondenes besvarelser stof til eftertanke.

Rapporten viser for eksempel, at 78 pct. af de adspurgte fonde primært bruger e-mail til at kommunikere med ansøgerne, ligesom 31 pct. af de adspurgte fonde videregiver ansøgninger til bestyrelsen via e-mail.

Men den udbredte brug af e-mail kan skabe problemer, understreger rapporten. E-mail kan blandt andet gøre det vanskeligt at holde styr på, hvordan personoplysninger spredes, ligesom fonden ved at bruge e-mail kan miste kontrollen over data:

"I disse tilfælde er det svært for fonden at sikre sig, at de får slettet en ansøgers personlige data fuldt ud og derved opfylder vedkommendes ret til at 'blive glemt'," står der i rapporten.

Og derfor kan et system, der gør det muligt at kommunikere uden brug af e-mail, være en styrke, fortæller direktør i Exformatics, Holger Foss:

"Et fondsadministrationssystem som vores er jo ikke lovpligtigt. Men hvis kommunikationen mellem ansøger, ansatte i sekretariatet og bestyrelsesmedlemmer, som sidder rundt om i industrien på hver sin arbejdsplads, foregår på e-mail og indeholder personlige oplysninger, så ligger der jo et sikkerheds-issue, som kan være utrolig svært at styre," siger Holger Foss.

Dyrt ikke at forholde sig til GDPR

Både Hanne Marie Motzfeldt, lektor i digital forvaltning ved Københavns Universitet, og Marlene Winther Plas, partner i advokatfirmaet DLA Piper, genkender rapportens overordnede billede.

"Det er ikke noget godt billede. Det er ikke betryggende. Men jeg er ikke overrasket," siger Hanne Marie Motzfeldt og fortsætter:

"Datatilsynet kommer ikke hylende og skrigende og flår fondene fra hinanden, hvis de bare opfører sig nogenlunde fornuftigt. Men det billede, jeg ser her, er ikke nogenlunde fornuftigt," siger Hanne Marie Motzfeldt.

Ifølge Hanne Marie Motzfeldt er det på tide, at fondene får styr på GDPR-reglerne. Ikke mindst er det vigtigt, at fondene bliver i stand til at dokumentere over for myndighederne, at de har forholdt sig til reglerne.

Hvis ikke fondene får bragt orden i sagerne, kan det nemlig koste mange penge.

"Fondene kan bare gå ind og se på Datatilsynets nyhed om firmaet ID Design. Firmaet manglede simpelthen at forholde sig til reglerne. Det havde ingen følsomme oplysninger liggende, hvilket ville have gjort sagen meget værre. Men firmaet blev alligevel indstillet til en bøde på 1,5 mio. kr.," siger Hanne Marie Motzfeldt.

Hanne Marie Motzfeldt understreger, at myndighederne har indført bøder i millionklassen for at opnå en afskrækkende virkning. Og at myndighederne ikke har noget problem med at lukke en fond eller en virksomhed med en millionbøde, hvis den ikke har styr på personoplysningerne og kan dokumentere det.

At man er en lille fond er ingen undskyldning for at lukke øjnene for GDPR-reglerne, understreger advokat og partner Marlene Winther Plas fra DLA Piper.

"Fra et GDPR-synspunkt er det ikke størrelsen af fonden, der er afgørende, men mængden af personoplysninger, der behandles og oplysningernes følsomhed. Mængden af personoplysninger vil typisk følge fondens størrelse, men oplysningernes følsomhed vil ikke," siger Marlene Winther Plas.

Ekspert: Fokusér på GDPRs tre bud

Lektor Hanne Marie Motzfeldt, der selv sidder i

bestyrelsen i to mindre fonde, medgiver, at GDPR-området kan være komplekst. Men hun mener, at fondene kan komme langt ved at forholde sig til de tre principper, som hun kalder GDPRs 'tre bud'.

"Personoplysninger må du kun behandle, hvis du har en god grund. Du må ikke luske, og du må ikke sjuske. Så enkelt kan de 99 GDPR-artikler egentlig siges. Og når jeg kigger på den her rapport, ser det ikke ud til, at fondene har forholdt sig til hjerteblodet i GDPR, nemlig de her tre bud," siger Hanne Marie Motzfeldt og fortsætter:

"Du skal til enhver tid kunne vise, at du har forholdt dig til de tre bud. Du skal kunne dokumentere det. Og det er dét, der kan gøre ondt. For du kan ikke tale dig ud af GDPR-reglerne, hvis myndighederne beder om at dokumentation," siger Hanne Marie Motzfeldt.

Om første bud siger Hanne Marie Motzfeldt:

"Du skal kun være i besiddelse af personoplysninger, hvis du har en god grund til det. Og dovenskab er ikke en god grund. Men at du skal behandle en ansøgning kan godt være en grund. GDPR åbner virkelig op for databrugen, men du er nødt til at forholde dig til, hvorfor du som fond har bestemte data, og hvad du gør med dem," siger Hanne Marie Motzfeldt.

Andet bud handler om, at fondene ikke må 'luske' med personoplysninger:

"Når folk giver dig personoplysninger, skal du være ærlig om, hvad du gør med oplysningerne. Det er fordi, man ønsker at skabe transparens i de enorme datastrømme, der findes digitalt. Så hvis du for eksempel har tænkt dig at videregive nogle af oplysningerne, så skal du fortælle folk det, allerede når de giver oplysningerne," siger Hanne Marie Motzfeldt.

Tredje bud handler om at undgå sjusk:

"Fondene skal lave en risikoanalyse, der forholder sig til, om det kan indebære nogen risiko for f.eks. ansøgerne at være registrerede. Hvis nogen søger om støtte til at sagsøge deres kommune, så er det jo ikke heldigt for dem, hvis det kommer ud i utide," siger Hanne Marie Motzfeldt.

Løsningen er ikke altid at købe en dims

Selvom et it-system kan være en hjælp, så løser det ikke alle problemer, understreger advokat Marlene Winther Plas fra DLA Piper:

"Indkøb af et it-system kan være et godt skridt på vejen mod at blive GDPR-compliant, men det er ikke nok i sig selv at købe et it-system, da fonden under alle omstændigheder skal tage forskellige aktive handlinger," siger hun.

Lektor Hanne Marie Motzfeldt er enig:

"Når jeg læser rapporten, virker det ikke som om, at fondene har tænkt de her tre bud igennem. Så bliver den nemme løsning måske at købe en dims i form af et it-system. Men det er ikke meningen med GDPR. Meningen er, at du skal forholde dig til de tre bud og tage dem alvorligt."

Og har man først gjort dét, så kan gratis værktøjer fra det offentlige faktisk udgøre et fint alternativ til både e-mail og mere komplekse it-systemer, siger Hanne Marie Motzfeldt:

"Fondene kan jo sende Digitaliseringsstyrelsen et julekort og sige tak for 'e-boks'. Tilgå informationerne dér. Det er simpelthen den nemmeste løsning, og det er drønsikkert. Det behøver ikke at være sværere," siger Hanne Marie Motzfeldt, der anbefaler at gå i gang med arbejdet straks:

"Sæt et punkt på næste bestyrelsesmøde om, at I skal have lavet et stykke arbejde for at forholde jer til de tre bud. I stedet for at kaste sig ud i at hyre konsulenter til mange hundrede tusinde kroner, så tag kontakt til andre fonde og find ud af, hvordan de har håndteret arbejdet. Der må vel være mulighed for at tage en dialog og dele noget materiale," slutter Hanne Marie Motzfeldt.

Rapporten fra Exformatics kan downloades her.

GDPR-RÅD

– fra Marlene Winther Plas, partner i advokatfirmaet DLA Piper

- Fonde, der behandler fortrolige eller følsomme oplysninger, eksempelvis fonde der kun uddeler midler, hvis ansøgeren har en bestemt sygdom, religion, etnicitet eller seksuel orientering, skal være forsigtige og sikre, at oplysningerne indsamles og opbevares lovligt.

- Fonde, der ikke bevidst indsamler følsomme oplysninger, skal også være opmærksomme, da ansøgere en gang imellem inkluderer følsomme oplysninger i en ansøgning, også uden at være opfordret hertil.

- Der skal kun indsamles de personoplysninger, som er relevante for behandling af ansøgninger

- Brug af CPR-nummer bør kun ske i det omfang, dette følger af anden lovgivning, og CPR-nummer bør ikke opbevares i længere tid, end hvad der er nødvendigt til dette formål. CPR-nummer bør derfor først indhentes, når dette er relevant. Fonde bør eksempelvis ikke bruge CPR-nummer som journalnummer.

- Oplysninger der ikke (længere) er relevante for ansøgningerne, skal slettes eller anonymiseres. Dette giver ofte anledning til udfordringer. For fonde, der behandler større mængder personoplysninger, er opsætning af automatiske sletterutiner tæt på at være den eneste fornuftige måde at håndtere dette på – i hvert fald på længere sigt.

- Fysisk opbevarede oplysninger er ikke altid omfattet af GDPR, men vil typisk være det for fonde, der eksempelvis opbevarer ansøgninger på struktureret vis i ringbind. Derudover kan fysisk opbevaring af oplysninger give anledning til en række sikkerhedsmæssige udfordringer, og disse bør derfor opbevares aflåst, hvis der er tale om følsomme personoplysninger.

- Hvis fonde bliver opmærksomme på, at personoplysninger om ansøgere er forkerte, skal oplysningernes rigtighed kontrolleres og berigtiges.

Fonde bør derfor som minimum udarbejde:

- En slettepolitik, som beskriver hvornår fonden sletter/anonymiserer personoplysninger modtaget fra ansøgere.

- En privatlivspolitik, som bl.a. beskriver hvorledes personoplysninger behandles, og hvilke rettigheder ansøgerne har i forhold til deres personoplysninger. Ansøgere skal blive gjort bekendt med privatlivspolitikken i forbindelse med ansøgningen.

- Databehandleraftaler med fondens underleverandører, herunder bl.a. administrator og IT-leverandører, hvor fonden instruerer databehandleren om behandling af personoplysningerne

- En datafortegnelse med en beskrivelse af, hvilke personoplysninger fonden modtager og behandler