



Årsberetning fra databeskyttelsesrådgiveren (DPO)

Gældende for perioden 1. januar 2022 – 31. december 2022

Opsummering

Ved udgangen af 2021 blev der truffet betydningsfulde beslutninger, som måtte forventes at sætte aftryk på mine opgaver i 2022. Disse forventninger er til fulde indfriet.

Beslutningerne var:

- Tilkøb af et system til understøttelse af informationssikkerhedsarbejdet i fagområderne
- Deltagelse i tværkommunalt samarbejde vedrørende tilsyn med databehandleraftaler
- Implementering af ny onboarding for nye ledere

At Nordfyns Kommunes initiativer fra 2021 var relevante og besluttet i tide blev bekræftet i forbindelse med besvarelsen af et skriftligt tilsyn fra Datatilsynet, som Nordfyns Kommune modtog den 30. august 2022. Nordfyns kommune var en af 54 kommuner og regioner, der modtog dette skriftlige tilsyn. Nordfyns Kommunes besvarelse af spørgsmålene blev markant mere positive, som følge af de ovenfor nævnte initiativer, om end Nordfyns Kommune stadig mangler meget, for at kunne dokumentere, at vi efterlever gældende regler.

Beslutningerne taler i nogen grad ind i min anbefaling fra sidste års beretning om, at Nordfyns Kommune med fordel kan arbejde for en mere centraliseret organisering af opgaverne tilknyttet GDPR og informations-sikkerhed generelt. Dette fordi fagområderne i højere grad end tidligere vil skulle løse opgaver efter central instruks, idet fagområderne ikke har de fornødne kompetencer til selv at tilrettelægge opgaverne på dette område. Der udestår dog stadig svar på, hvordan opgaverne i praksis vil blive løst i de enkelte fagområder.

Indhold

Implementering af ledelsessystem	3
Deltagelse i det fælleskommunale Databehandlersekretariat (DBS).....	3
Implementering af ny onboarding for nye ledere	4
Organisatorisk styrkelse af støtte til fagområderne	4
Tilsyn og sikkerhedsbrud	5
Bøder fra Datatilsynet i 2022	6
Vurdering af GDPR lovmedholdelighed i Nordfyns Kommune	7

Implementering af ledelsessystem

Nordfyns Kommune har købt adgang til systemet Wired Relations, med henblik på, at sikre nødvendig understøttelse til fagområdernes opgavehåndtering i forhold til GDPR og informationssikkerhed. Kontrakten blev indgået i februar 2022, og herefter fulgte opsætning og instruktion i betjening af systemet, som Informationssikkerhedsteamet indledningsvist har været ansvarlig for.

Wired Relations er primært et procesunderstøttende system, som sikrer påmindelse om opgaver, som den ansvarlige skal løse. Derudover sikrer systemet den nødvendige dokumentation for, at de ansvarlige har taget stilling til hver enkelt opgave. Denne dokumentation er afgørende for, at Nordfyns Kommune kan leve op til kravene i forhold til GDPR og informationssikkerhed.

Implementeringen af systemet i fagområderne følger udrulningen af Nordfyns Kommunes rolle- og rettighedsstyringssystem (IDM). Begge dele har sikkerhed og GDPR som hovedformål, og det giver derfor god mening, at lade disse to ting følges af. Udrulningen af Wired Relations blev derfor udskudt til ultimo 2022, og forventes afsluttet ultimo 2023.

Deltagelse i det fælleskommunale Databehandlersekretariat (DBS)

I maj måned 2022 tiltrådte Nordfyns Kommune Det Fælleskommunale Databehandlersekretariat (DBS), som har til formål at føre tilsyn med databehandlere, som anvendes af minimum 20 medlemskommuner. I skrivende stund er 62 kommuner medlem af DBS.

Databehandlersekretariatet overtager ikke det juridiske ansvar forbundet med tilsynet, men sparer kommunerne for en stor praktisk opgave hermed. Når tilsynsrapporten foreligger mangler blot en formel godkendelse, som Informationssikkerhedsteamet står for i samarbejde med den systemansvarlige chef eller leder.

Som nævnt varetager Databehandlersekretariatet kun tilsynet for de databehandlere, som anvendes af minimum 20 medlemskommuner. Dermed mangler der fortsat håndteringen af tilsyn for de få databehandlere, som anvendes af mindre end 20 medlemskommuner. Ansvar for tilsyn med disse sorteres fortsat under den systemansvarlige chef eller leder.

Ud over at føre tilsyn med databehandlere, vil Databehandlersekretariatet på sigt også kunne forhandle nye databehandleraftaler på plads på kommunernes vegne. Dette forventes at kunne bringe kommunerne i en bedre forhandlingsposition fremadrettet.

Kontakten mellem Nordfyns Kommune og Databehandlersekretariatet er naturligt forankret i databeskyttelsesrådgiverfunktionen.

Implementering af ny onboarding for nye ledere

Som noget nyt er Databeskyttelsesrådgiveren nu en fast del af onboarding af nye ledere i Nordfyns Kommune. Sammen med It-arkitekten afholdes der et møde for nye ledere hver 2. måned, hvor de nyansatte ledere introduceres til deres ansvar forbundet med GDPR, informationssikkerhed og IT generelt.

Initiativet er endnu ikke evalueret, men vurderes absolut relevant, set fra et GDPR perspektiv. Lederne modtager nødvendig viden om deres rolle og ansvar i forhold til GDPR og informationssikkerhed, samt viden om hvem de kan spare med om spørgsmål hertil. Derudover kommer der værdifuld viden retur, i form af ideer fra andre ansættelsesforhold eller forventninger til os, som kan afstemmes på stedet.

Initiativet kunne med fordel videreudvikles således, at det ikke kun er nyansatte ledere, der møder DPO i forbindelse med onboarding, men også nyansatte sagsbehandlere. Initiativet kunne muligvis digitaliseres, således at resurstrækket forbundet hermed reduceres. Initiativet kan med fordel dokumenteres i forhold til deltagere, hvorved kommunen også sikrer dokumentation for awareness i denne forbindelse. Disse perspektiver videregives ligeledes, når initiativet bliver evalueret.

Organisatorisk styrkelse af støtte til fagområderne

Siden min ansættelse som DPO i Nordfyns Kommune i januar 2021 har jeg haft fokus på at sikre en hensigtsmæssig organisering og opgaveløsning i forhold til informationssikkerhed generelt. Årsagen til dette fokus er, at den rette organisering og prioritering vil sikre størst mulige effekt (lovmedholdelighed) ved brug af færrest mulige resurser. Nordfyns Kommune er decentalt organiseret, hvilket betyder, at der kun er ganske få centrale resurser til rådighed for bistand og support. En succesfuld løsning af opgaverne med denne organiseringsform forudsætter, at decentrale enheder har flere resurser med et højere kompetenceniveau til rådighed. Dette er ikke tilfældet for Nordfyns Kommune.

Der er ikke nogen specifikke formkrav til, hvor mange resurser en kommune skal afsætte til dette område. Persondataforordningen beskriver dog, at den dataansvarlige skal sikre passende tekniske og organisatoriske foranstaltninger, for at være i stand til at påvise at være i overensstemmelse med forordningen (artikel 24, stk. 1). Sammenlignet med de andre fynske kommuner, ligger Nordfyns Kommune meget lavt i forhold til prioritering af resurser. Kun Ærø og Langeland kommuner har afsat færre resurser. Det er derfor min vurdering, at Nordfyns Kommunes risikoprofil er høj, som konsekvens af denne lave resurseprioritering, idet vi vil have flere mangler og lave flere fejl som følge heraf.

I min årsberetning fra 2021 adresserede jeg første gang denne udfordring. Derfor var det min ambition for 2022, at motivere organisationen til en anderledes organisering og prioritering af området. Jeg havde i den forbindelse et punkt på Strategisk Chefforum, med resurser og prioritering som tema. Af drøftelserne under punktet udleder jeg, at fagområderne i høj grad har behov for og ønsker at kunne modtage meget mere støtte og hjælp til opgaverne, men at det ikke på nuværende tidspunkt er praktisk muligt at organisere eller prioritere anderledes.

Status for dette punkt er derfor, at Nordfyns Kommune fortsat kun har få centrale resurser til rådighed for håndteringen af opgaveløsningen i forhold til GDPR og informationssikkerhed. Dette forhold udgør en væsentlig organisatorisk risiko, som jeg igen i år, må anbefale reduceret, idet enhver uløst opgave udgør en risiko for den registrerede.

Tilsyn og sikkerhedsbrud

Nordfyns Kommune har to gange været i Datatilsynets søgelys i 2022. Først og fremmest i forbindelse med den nationale sag om brug af Chromebook på skoleområdet, og senest i forbindelse med ovenfor omtalte skriftlige tilsyn fra august 2022.

Sagens om brug af Chromebook har jeg fulgt på sidelinjen, idet Nordfyns Kommune overgav den nationale del af håndteringen til KL. Den rent kommunale del af opgaven er håndteret i tæt samarbejde mellem IT-arkitekten og skoleområdets IT-konsulent. Jeg er løbende blevet orienteret om arbejdet, som jeg vurderer er løst bedst muligt, set i forhold til de kompetencer og resurser Nordfyns Kommune har haft til rådighed. Derudover høstes der erfaringer fra opgaven, som danner grundlag for løsningen af lignende opgaver fremadrettet, herunder fx udarbejdelse af risikovurderinger.

Det skriftlige tilsyn fra august 2022 har jeg derimod været tæt involveret i besvarelsen af. Dels fordi det giver mening, at jeg som DPO lader min opfattelse af kommunens modenhedsniveau afspejle sig i svarene, og dels fordi min viden herom er forholdsvis omfattende.

Som ovenfor nævnt blev besvarelsen af det skriftlige tilsyn markant mere positiv som følge af de beslutninger, som blev taget i slutningen af 2021, og ligeledes på grund af beslutningen om at godkende en nye udgave af Politik for Informationssikkerhed (Godkendt på kommunalbestyrelsesmødet den 27. oktober 2022 punkt 177). Årsagen til dette er, at vi på baggrund af disse beslutninger nu kunne besvare en hel del spørgsmål med "i gang" i modsætning til "ikke i gang". Dette må antages at være en væsentlig årsag til, at Datatilsynet for nuværende har lukket det skriftlige tilsyn for så vidt angår Nordfyns Kommune.

Sikkerhedsbrud

I 2022 har der været 15 anmeldte sikkerhedsbrud samt 2 hændelser, som ikke er anmeldt. Et sikkerhedsbrud – en uberettiget videregivelse af personoplysninger til uvedkommende - skal som altovervejende hovedregel anmeldes til Datatilsynet. Vi kan kun undlade anmeldelse, hvis

bruddet ikke kan tænkes at udløse en risiko for den registrerede. Datatilsynets fortolkning af, hvad der kan udløse en risiko er meget stram, hvilket betyder at stort set alle hændelser skal anmeldes. Endnu har ingen af de anmeldte sikkerhedsbrud i 2022 ført til andet end kritik. To sager mangler dog at blive afsluttet, men ingen af dem forventes at føre til andet end kritik. Alle anmeldelser af sikkerhedsbrud modtages som minimum kritik.

8 af de 15 sikkerhedsbrud er sket på Børn og Unge område, hvilket jeg ser som et udtryk for, at medarbejderne ved Børn og Unge besidder passende viden om, hvornår der er sket et sikkerhedsbrud og hvordan sådanne situationer skal håndteres. Modsætningsvis bekymrer det mig, at der ikke er en eneste registreret hændelse ved Arbejdsmarked og kun en enkelt ved Sundhed og Rehabilitering som i lige så høj grad arbejder med personoplysninger. Jeg vil forholde mig nysgerrigt til dette i 2023 og inddrage mine bekymring i forhold til videreudviklingen af awareness for GDPR og informationssikkerhed.

Det var min forventning, at den awareness kampagne, som blev udrullet over det meste af organisationen i 2021, ville kunne afspejle sig i antallet af anmeldte sikkerhedsbrud for 2022. Dette var ikke tilfældet. Til sammenligning var der 12 indberettede sikkerhedsbrud i 2021 og 3 hændelser, som ikke blev indberettet. Hvilke tiltag denne manglende udvikling i antallet af sikkerhedsbrud eventuelt skal udløse, vil blive drøftet i Informationsikkerhedsudvalget, idet det ganske simpelt er urealistisk, at der slet ikke laves fejl ved Sundhed og Rehabilitering og stort set heller ikke på Arbejdsmarkedsområdet.

Fejl vil ske, og når de sker, er der beskrevet en let og hurtig proces til fagområderne på intranettet. Fagområdet skal blot udfylde et kort skema med nødvendige oplysninger om det, der er sket, og sende det til DPO@nordfynskommune.dk, hvorefter jeg sørger for indberetning og opfølgning. Kun i tilfælde af større og komplicerede brud, kan der være behov for yderligere undersøgelser ved fagområdet.

Samlet statistik over anmeldte sikkerhedsbrud:

Børn og Unge	8
Teknik, Erhverv og Kultur	2
Sundhed og rehabilitering	1
Økonomi og Løn	2
Generelle	2

De to hændelser, som ikke blev anmeldt, var henholdsvis fra Børn og Unge og fra Teknik, Erhverv og Kultur.

Bøder fra Datatilsynet i 2022

Datatilsynet har indstillet 3 offentlige myndigheder til bøde i 2022, herunder en enkelt kommune.

Indstillingen til bøde for den pågældende kommune skyldtes, at de ansatte i kommunen kunne slå deres adgangskode fra på telefoner og tablets. Dette forhold har givet Datatilsynet anledning til at politianmelde kommunen, fordi borgerne derved blev udsat for en unødigt risiko. Bøden er indstillet til 50.000 kr.

Datatilsynet udtaler om indstillingen, at telefoner og tablets af og til bliver stjålet, tabt eller glemt, og hvis uvedkommende uden videre kan få adgang til de oplysninger, der er på dem, lever man ikke op til sit ansvar.

Datatilsynet lagde endvidere vægt på, at den dataansvarlige må påregne, at ikke alle ansatte til enhver tid vil følge interne retningslinjer om brug af koder. Derfor skal der sikres en reel beskyttelse (teknisk beskyttelse) der, hvor det er muligt, således at misbrug undgås i videst muligt omfang. [Læs om afgørelser ved Datatilsynet](#)

Ud fra denne sag er det min anbefaling, at Nordfyns Kommune i sit fremadrettede arbejde med sikkerhed omkring persondata, sørger for at have en så teknisk sikker opsætning som muligt, idet en klar retningslinje for korrekt behandling heraf, ikke er tilstrækkeligt.

Vurdering af GDPR lovmedholdelighed i Nordfyns Kommune

Som DPO vurderer jeg, at Nordfyns Kommune mangler meget for at kunne dokumentere efterlevelse af reglerne i persondataforordningen og anden relevant regulering på området, men at der er foretaget positive fremskridt i forhold til på sigt at kunne blive lovmedholdelig. Det er min vurdering, at der må tilføres flere ressourcer til opgaverne, centralt eller decentralt, hvis Nordfyns Kommune skal lykkes med at blive lovmedholdelig.