# Årsberetning fra databeskyttelsesrådgiveren (DPO)

Gældende for perioden 1. januar 2023 – 31. december 2023

## Indledning

Databeskyttelsesrådgiveren (i det følgende benævnt DPO) har til opgave at rådgive kommunen og hjælpe til med at kommunen efterlever de databeskyttelsesretlige regler.

Databeskyttelsesrådgiveren skal én gang årligt afgive rapport til det øverste ledelsesniveau.

## Opsummering

Nordfyns Kommunes organisering af opgaver og ansvar i forhold til arbejde forbundet med GDPR, har været mit fokus siden min ansættelse som DPO i Nordfyns Kommune 1. januar 2021. Dette fordi en hensigtsmæssig organisering har stor betydning for om og hvordan opgaverne løses. Det er min vurdering, at den nuværende organisering i Nordfyns Kommune vedr. GDPR i begrænset omfang understøtter opgaveløsningen under GDPR (Generel Data Protektion Regulation).

I Nordfyns Kommune er fagområderne som udgangspunkt ansvarlige for opgavevaretagelsen under GDPR med mulighed for support fra stabene. En sådan organisering forudsætter stor lokal viden om opgaver og ansvar, samt et højt niveau for sammenstilling af oplysninger om compliance (lovmedholdelighed) til brug for den centrale ledelse i kommunen. Dette med henblik på, at oplysningerne kan anvendes i forbindelse risikovurderinger i forhold til kommunens samlede ansvarsforhold.

På baggrund af mine årsberetninger fra 2021 og 2022 samt mine erfaringer fra 2023, er det min anbefaling, at Nordfyns Kommune revurderer organiseringen af opgaver og ansvar forbundet med GDPR, idet disse kun i begrænset omfang passer til den generelle organisering. Sammenhængende hermed anbefaler jeg større fokus på GDPR-compliance generelt i Nordfyns Kommune, hvilket dog forventes af komme naturligt ved en beslutning om, at revurdere organiseringen i forhold til opgaver og ansvar under GDPR.

<u>Afgrænsning</u>

Denne rapport vedrører alene de organisatoriske forhold vedrørende GDPR-compliance. Det skyldes, at de tekniske forhold er af fortrolig karakter. Administrationen udarbejder et særskilt notat om disse forhold.



Sagsnummer: S2023-15023
Dokumentnummer: D2023-36821
Afdeling: Strategi og Politik
Udarbejde af: Databeskyttelsesrådgiver, Birgit Mia Larsson

# Indhold

## 1. Implementering af processtyringssystem

I februar 2022 købte Nordfyns Kommune adgang til processtyringssystemet Wired Relations, med henblik på at sikre nødvendig understøttelse af Nordfyns Kommunes opgavehåndtering og dokumentation herfor i forhold til GDPR og informationssikkerhed. Systemet sammenstiller informationer til ledelsen om kommunens samlede risikoprofil i forhold til informationssikkerhed.

Siden februar 2022 har Informationssikkerhedsteamet anvendt systemet intensivt. Udrulningen af systemet til brug i fagområderne var planlagt i 2023, men udrulningen udestår desværre fortsat, hvilket skyldes manglende resurser til opgaven centralt og decentralt.

Oprindeligt var udrulningen planlagt til at følges med implementeringen af et nyt IDM system. Denne implementering trak dog ud og endte med at blive aflyst medio 2023, til fordel for et andet og bedre IDM system.

Betydning af manglende implementering
Det er ikke afgørende for overholdelsen af GDPR, at organisationen har et system til understøttelse af opgaveløsningen og sammenstilling af oplysninger til ledelsen. Et system som Wired Relations sikrer dog et kontinuerligt fokus for opgaveløsning og prioritering af resurser hertil på et oplyst grundlag. Disse oplysninger vil være overordentligt resursekrævende at tilvejebringe uden systemunderstøttelse, hvis Datatilsynet efterspørger dokumenteret status på overholdelsesniveauet i henhold til GDPR fra Nordfyns Kommune. (Fokusområde for Datatilsynet i 2024)

Når Wired relations er fuldt ud implementeret og operationelt vil Nordfyns Kommunes ledelse centralt som decentralt kunne gøre sig bekendt med status og risikoprofil løbende, og dermed have tilstrækkelig viden til at enten at acceptere risikoprofilen eller at iværksætte relevante initiativer, så risikoprofilen kan blive acceptabel. Uden et sådan overblik, risikerer ledelsen af prioritere uden tilstrækkelig indsigt.

Anbefaling:
Idet fagområderne opnår overblik over opgaveporteføljen, indsigt i status herpå samt viden om fagområdets compliance-niveau, anbefales det, at Nordfyns Kommune prioriterer fuld implementering og fremadrettet betjening af det indkøbte procesunderstøttelsessystem, Wired Relations.

## 2. Deltagelse i det fælleskommunale Databehandlersekretariat (DBS)

I maj måned 2022 tiltrådte Nordfyns Kommune Det Fælleskommunale Databehandlersekretariat (DBS). Oprindeligt var formålet med DBS at føre tilsyn med kommunernes databehandlere, som anvendes af minimum 20 medlemskommuner. I 2023 har DBS udvidet deres opgavefelt på to betydningsfulde punkter:

- Der skal kun 10 kommuner til, som anvender databehandleren, før DBS påtager sig tilsynet med databehandleren.
- DBS påtager sig i stigende grad også at forhandle databehandleraftaler på plads for kommunerne. DBS prioritere denne opgave ud fra, om de har kapacitet til opgaven. Er der kapacitet, prioriteres de opgaver, som kommer flest medlemskommuner til gavn.

Det er min vurdering, at Nordfyns Kommune med sit medlemskab sikrer varetagelsen af tilsyn med databehandlere svarende til 90 %. Det bemærkes, at opgaverne er ens for alle kommuner, og at det derfor giver god mening, resursemæssigt som økonomisk, at kommunerne

arbejder sammen om at løse opgaven.

De 10% af opgaven som fortsat udestår, består dels af godkendelse af tilsynene, udarbejdelse af ledelseserklæringer til hvert tilsyn samt naturligvis tilsyn med de få databehandlere, som DBS ikke tager sig af. Ansvaret for disse opgaver ligger i fagområderne og opgaverne procesunderstøttes af Wired relations som beskrevet overfor under punkt 1.

Anbefaling:
Idet håndteringen af de sidste 10% af opgaverne er forbundet med revision af databehandlere der systemunderstøttes af Wired Relations, henvises der til anbefalingen under punkt 1.

Det bemærkes, at Datatilsynet ikke godkender tilsyn foretaget af DBS, uden en underskrevet ledelseserklæring på baggrund af tilsynet. Opgaven med at udarbejde disse ledelselserklæringer følger implementeringen af Wired Relations.

## 3. Onboarding af nye ledere

Databeskyttelsesrådgiveren har i 2023 været en fast del af onboarding af nye ledere i Nordfyns Kommune. Sammen med It-arkitekten afholdes der et møde for nye ledere ca. hver 2. måned, hvor de nyansatte ledere introduceres til deres ansvar forbundet med GDPR, informationssikkerhed og IT generelt. Der ud over skal alle nye ledere gennemgå et digitalt kursus i GDPR inden for de første 30 dage af ansættelsen.

Anbefaling:
Initiativet med awarenes i forbindelse med onboarding kan med fordel videreudvikles således, at også nyansatte sagsbehandlere møder DPOén i forbindelse med onboarding. Vælger Nordfyns Kommune at følge denne anbefaling, vil initiativet med fordel kunne digitaliseres, således resursetrækket bliver minimalt, samtidig med at formålet opfyldes. En digitaliseret model kan ligeledes sikre systematisk dokumentation herfor.

## 4. Organisatoriske forhold

Siden min ansættelse som DPO i Nordfyns Kommune i januar 2021 har jeg haft fokus på Nordfyns Kommunes organisering forbundet med opgaveløsningen i forhold til efterlevelse af GDPR. Dette fordi der ikke synes at være sammenhæng mellem ansvar og kompetencer, samt at der ikke syntes at være tilstrækkelige resurser til rådighed i forhold til opgavemængde. Disse udfordringer opleves relevante centralt som decentralt, jf. også punkt 1 ovenfor.

Som følge heraf løfter fagområderne ikke i tilstrækkelig grad deres ansvar i henhold til GDPR. Fagområderne kan ikke modtage tilstrækkelig central støtte dertil, idet der også her er for få resurser til rådighed. Indkøb af Wired Relations og deltagelsen i DBS er begge initiativer som på hver deres måde har til formål at understøtte dele af Nordfyns Kommunes opgaveportefølje under GDPR, men det er ikke tilstrækkeligt. Der mangler fortsat tydelig lokal forankring af de opgaver, der nødvendigvis skal løftes lokalt i fagområderne og resurser til varetagelse af de opgaver, der bedst håndteres centralt. Derudover kunne opgavefordelingen med fordel ændres, således der i højere grad er sammenhæng mellem opgaver og kompetencer.

I september 2022 deltog databeskyttelsesrådgiveren på Strategisk Chefforum, hvor fagområdernes opgaver blev belyst. Dette i forbindelse med forberedelser af implementering af Wired Relations. Som nævnt ovenfor er det endnu ikke lykkedes at implementere Wired Relations til fagområderne, hvorfor jeg i efteråret 2023 tog på rundtur i fagområderne for endnu en gang at belyse fagområdernes overordnede opgaver. Mit formål med rundturen var, at motivere til dialog om, hvordan opgaverne kan løses fremadrettet.

<u>Rette organisering</u>
"Den rette organisering og prioritering vil sikre størst mulige effekt (lovmedholdelighed) ved brug af færrest mulige resurser". (Citat fra årsberetningen for 2022). Persondataforordningen forholder sig dog ikke til, hvordan den dataansvarlige organiserer sig i praksis, men angiver blot at den dataansvarlige skal sikre passende tekniske og organisatoriske foranstaltninger.

De organisatoriske foranstaltninger rummer blandt andet, at man skal organisere sig på en måde, der understøtter overholdelse af persondataforordningen. Som ovenfor beskrevet, der det min opfattelse, at Nordfyns Kommune på nuværende tidspunkt ikke har en organisering, der i tilstrækkelig grad understøtter overholdelse af persondataforordningen, idet der ikke er sammenhæng mellem opgaver, kompetencer og resurser.

Det bemærkes i øvrigt, at Nordfyns Kommunes tekniske foranstaltninger, som i høj grad løftes centralt, historisk set har været højere prioriteret. Derfor er Nordfyns Kommune bedre stillet i forhold til de tekniske foranstaltninger, end tilfældet er for de organisatoriske.

<u>Anbefaling:</u>
Nordfyns Kommune anbefales at revurdere organiseringen af opgaver og ansvar under GDPR, med henblik på, at udnytte de tilstedeværende resurser og kompetencer optimalt, samt at sikre nødvendigt tilførsel af tilstrækkelige resurser hertil fremadrettet.

En revurdering kunne ske ved nedsættelse af en arbejdsgruppe, hvis formål kunne være at anbefale en hensigtsmæssig opgaveorganisering under GDPR med udgangspunkt i Nordfyns Kommunes generelle organisering. Arbejdsgruppen kunne med fordel belyse mangler som

følge af den anbefalede organisering, således direktionen på et oplyst grundlag kan tage stilling til, hvordan opgaverne fremadrettet skal håndteres og prioriteres.

## 5. Sammenlægning af Informationssikkerhedsudvalget og Digitaliseringsudvalget

Den 19. december 2023 drøftede medlemmerne af Informationssikkerhedsudvalget og Digitaliseringsudvalget, mulighederne for at lægge de to udvalg sammen. Opgavesammenfald og sammenfald af medlemmer i de to udvalg er over tid blevet markant, hvorfor fordelene ved en sammenlægning var væsentlige, sammenholdt med at en fortsat opdeling vil være unødigt ressourcekrævende for de medlemmer, der er knyttet til begge udvalg.

Den 10. januar 2024 godkendte direktionen sammenlægningen af de to udvalg. Fremadrettet vil alle væsentlige emner vedrørende digitalisering, informations- og cypersikkerhed blive drøftet i Udvalg for digitalisering og informationssikkerhed.

Som DPO har jeg hidtil kun haft en plads i et af de to nu sammenlagte udvalg. Jeg hilser derfor initiativet velkomment og ser frem til at blive inddraget yderligere under den nye organisering.

## 6. Tilsyn og sikkerhedsbrud

Nordfyns Kommune har modtaget to tilsynshenvendelser fra Datatilsynet i 2023. Begge var af generel karakter.

I marts måned modtog kommunen et tilsyn vedrørende databeskyttelsesrådgiverens rolle og udpegelse. Formålet med dette tilsyn var, at afklare, hvorvidt der er behov for at udarbejde en vejledning til kommunerne herom. Tilsynet har ikke givet anledning til konkrete handlinger i Nordfyns Kommune.

I maj måned 2023 modtog kommunen endnu et skriftligt tilsyn. Denne gang vedrørende kommunens brug af AI-løsninger. Nordfyns Kommune anvendte endnu ikke AI-løsninger på daværende tidspunkt, hvorfor dette tilsyn heller ikke gav anledning til yderligere.

<u>Sikkerhedsbrud</u>
I 2022 har der været 31 sager om sikkerhedsbrud, hvoraf 21 er anmeldt til Datatilsynet. Et sikkerhedsbrud er en uberettiget videregivelse af personoplysninger til uvedkommende, og det skal som altovervejende hovedregel anmeldes til Datatilsynet. Vi må dog undlade at anmelde hændelsen, hvis en egentlig risiko for den registrerede er usandsynlig. Datatilsynets fortolkning af, hvad der kan udgøre en risiko for den registrerede er meget stram, hvilket betyder at langt de fleste hændelser må forventes at skulle anmeldes. Alle anmeldte sikkerhedsbrud i 2023 har ført til ”kritik”, hvilket er Datatilsynets mildeste reaktion.

Fejl vil ske, og når de sker, er det afgørende, at man handler ansvarligt og ordentligt. Medarbejderen skal orientere nærmeste leder om hændelsen, og udfylde et kort skema med nødvendige oplysninger om det, der er sket, og sende det til DPO@nordfynskommune.dk, hvorefter DPO sørger for indberetning til Datatilsynet. Kun i tilfælde af større og komplicerede brud, vil der være behov for yderligere undersøgelser ved fagområdet.

Når fejl sker, er det vigtigt at vi alle lærer af dem. Vi skal have mod til at tale højt om de fejl vi begår. Jo mere vi tør stå ved vores fejl, jo større sandsynlighed er der for, at vi kan lykkedes med at tage ved lære heraf og dermed blive bedre i fremtiden.

*Børn og Unge*
11 sikkerhedsbrud er registreret ved Børn og Unge. Det er 3 sager mere end i 2022. Det er positivt, at der er flere anmeldelser i 2023, men det er fortsat et lavt tal.

*Arbejdsmarked*
5 Sikkerhedsbrud er registreret ved Arbejdsmarked i 2023. Til sammenligning var der ikke et eneste i 2022. De fleste af disse sikkerhedsbrud er dog af teknisk karakter og dermed indberettet via systemleverandør. Dermed bekymrer det fortsat, at der indberettes så få sikkerhedsbrud fra dette fagområde.

*Sundhed og rehabilitering*
4 Sikkerhedsbrud er indberettet i 2023, hvilket er 3 flere end i 2022. Også her har der været sikkerhedsbrud af teknisk karakter fra systemleverandør. Dermed bekymrer det fortsat, at der indberettes så få sikkerhedsbrud fra dette fagområde.

*Teknik, Erhverv og Kultur*
Der er registreret 4 sikkerhedsbrud, hvilket er 2 mere end i 2022. Teknik, Erhverv og Kultur anvender hovedsageligt almindelige personoplysninger og dette i mindre omfang end de øvrige fagområder, hvorfor det er forventet, at dette fagområde har færre indberetninger af sikkerhedsbrud.

*Stabene*
Der er registreret 7 sikkerhedsbrud for staben mod 2 i 2022. Det skal for stabene bemærkes, at opgaverne her, ikke indeholder beskyttede personoplysninger i samme grad som de øvrige fagområder, hvorfor det er forventet, at dette fagområde har færre indberetninger af sikkerhedsbrud. Dertil kommer, at der er flere generelle anmeldelser af sikkerhedsbrud fra systemleverandører af tværfaglige systemer. Disse sikkerhedsbrud tilfalder stabene, da systemansvaret for tværfaglige systemer varetages her.

Samlet statistik over anmeldte sikkerhedsbrud:

| | |
|---|---|
| Børn og Unge | 11 |
| Arbejdsmarked | 5 |
| Sundhed og rehabilitering | 4 |
| Teknik, Erhverv og Kultur | 4 |
| Stabene | 7 |

Anbefaling:

Nordfyns kommune ligger stadig meget lavt i forhold til antal sikkerhedsbrud, hvorfor det anbefales at Nordfyns Kommune har fokus på vidensdeling og oplysning herom i 2024. Som DPO vil jeg understøtte dette initiativ på egen hånd internt. Dog vil det have mærkbart større effekt, hvis ledelsen tager ansvar for vidensdeling og oplysning om emnet til medarbejderne direkte.

## 7. Nyt fra Datatilsynet i 2023, og planer for 2024

2023 har ikke budt på markante udtalelser til kommunerne. Derimod har statslige institutioner modtaget flere kritiske udtalelser. Særligt digitaliseringsstyrelsen har modtaget kritik flere gange gennem året.

Temaerne for kritikken af offentlige institutioner i 2023 har været følgende:

- Samtykke, og hvad det kan bruges til, når det gives til en offentlig myndighed
- Utilstrækkelig risikovurdering
- Behandling af flere oplysninger end nødvendigt
- Manglende sikkerhedsforanstaltninger
- Manglende test og kontrol af brugeradgange

Datatilsynets fokusområder i 2024, som forventes at kunne berøre kommunerne er:

- Brug af kunstig intelligens og automatisering
- Overvågning af ansatte
- Den registreredes ret til indsigt
- Kommunale webarkiver
- Online og fysiske indkøb
- Rettighedsstyring og forebyggelse af misbrug af adgang til personoplysninger
- Grundlæggende behandlingssikkerhed hos kommuner og regioner

## 8. Vurdering af GDPR lovmedholdelighed i Nordfyns Kommune

På baggrund af ovenstående er det min vurdering, at Nordfyns Kommune stadig har væsentlige mangler på det organisatoriske område, i forhold til at kunne dokumentere efterlevelse af reglerne i persondataforordningen. Det er min vurdering, at der må prioriteres resurser til opgaverne, hvis Nordfyns Kommune skal lykkedes med at løse alle opgaver under GDPR i tilstrækkelig grad.

## 9. Anbefalinger – samlet og i prioriteret rækkefølge

Anbefalingerne fra denne årsberetning bør prioriteres i forhold til relevans, sammenhæng forventet effekt.

1. prioritet - vedrørende organisatoriske forhold, afsnit 4:
*"Nordfyns Kommune anbefales at revurdere organiseringen af opgaver og ansvar under GDPR, med henblik på, at udnytte de tilstedeværende resurser og kompetencer optimalt, samt at sikre nødvendigt tilførsel af tilstrækkelige resurser hertil fremadrettet. En revurdering kunne ske ved nedsættelse af en arbejdsgruppe, hvis formål kunne være at anbefale en hensigtsmæssig opgaveorganisering under GDPR med udgangspunkt i Nordfyns Kommunes generelle organisering. Arbejdsgruppen kunne med fordel belyse mangler som følge af den anbefalede organisering, således direktionen på et oplyst grundlag kan tage stilling til, hvordan opgaverne fremadrettet skal håndteres og prioriteres*."

Gennemførsel af denne anbefaling vil sikre optimal opgavefordeling og kvalitativ belysning af resursebehov, hvorefter ledelsen vil kunne træffe en oplyst beslutning om, hvordan opgaverne skal løses fremadrettet. Dette skridt er afgørende for, at Nordfyns Kommune fremadrettet vil kunne løfte opgaverne under GDPR i tilstrækkeligt omfang.

2. prioritet – Implementering af procesunderstøttelsessystemet, afsnit 1 og 2:
Afsnit 1: *"Idet fagområdernes opnår overblik over opgaveporteføljen, indsigt i status herpå samt viden om fagområdets compliance-niveau, anbefales det, at Nordfyns Kommune prioriterer fuld implementering og fremadrettet betjening af det indkøbte procesunderstøttelsessystem, Wired Relations*".

og

Afsnit 2: *"Idet håndteringen af de sidste 10% af opgaverne forbundet med revision af databehandlere systemunderstøttes af Wired Relations, henvises der til anbefalingen under punkt 1. Det bemærkes, at Datatilsynet ikke godkender tilsyn foretaget af DBS, uden en underskrevet ledelseserklæring på baggrund at tilsynet. Opgaven med at udarbejde disse ledelseserklæringer følger implementeringen af Wired Relations*".

Disse to anbefalinger bør følges, når der er klarhed over, hvor opgaverne i systemet skal håndteres, jf. anbefalingen med 1. prioritet.

3. prioritet – sikkerhedsbrud, afsnit 6:
"Nordfyns kommune ligger stadig meget lavt i forhold til antal sikkerhedsbrud, hvorfor det anbefales at Nordfyns Kommune har fokus på vidensdeling og oplysning herom i 2024. Som DPO vil jeg understøtte dette initiativ på egen hånd internt. Dog vil det have mærkbart større effekt, hvis ledelsen tager ansvar for vidensdeling og oplysning om emnet til medarbejderne direkte".

Det er min forventning, at denne anbefaling løftes indirekte, såfremt ovenstående anbefalinger følges. Dette som et naturligt følge af, at der med ovenstående initiativer kommer større fokus og dermed større ansvarsfølelse i forhold til efterlevelsen af GDPR. Dertil skal lægges, at

effekten heraf må forventes at blive markant større, hvis initiativet udsættes til efter implementering af de to første anbefalinger.

4. prioritet – onboarding af nye medarbejdere, afsnit 3:
"Initiativet kan med fordel videreudvikles således, at det ikke kun er nyansatte ledere, der møder DPO i forbindelse med onboarding, men også nyansatte sagsbehandlere. Vælger Nordfyns Kommune at følge denne anbefaling, vil initiativet med fordel kunne digitaliseres, således ressursetrækket bliver minimalt samtidig med at formålet opfyldes. En digitaliseret model kan ligeledes sikre dokumentation for awarenes i forhold til de nyansatte".

Dette initiativ vedrører awarenes, som kan løses på mange forskellige måder. Metoden er derfor ikke afgørende for, om kommunen er complient i forhold til GDPR, og kan derfor med fordel udskydes til efter implementeringen af de højere prioriterede opgaver.