norddjurs kommune

DATABESKYTTELSES-RÅDGIVERENS ÅRSRAPPORT 2023

April 2024

Indhold

1. Indledning 3

2. Formål 3

3. Metode 3

4. Databeskyttelsesrådgiveren i Norddjurs Kommune 3

5. Det forgangne år – 2023 3

5.1 Status på anbefalinger til fokusområder i det forgangne år 3
5.2 Andre fokusområder i det forgangne år 5
5.3 Sikkerhedshændelser og -brud 5

6. Anbefalinger til fokusområder i 2024 6

6.1 Datatilsynets anbefalinger til fokusområder i 2024 6
6.2 Databeskyttelsesrådgiverens anbefalinger til fokusområder i 2024 7

7. Konkluderende bemærkninger 8

1. Indledning

Databeskyttelsesrådgiverens årsrapport er den årlige rapportering af Norddjurs Kommunes arbejde med informationssikkerhed og databeskyttelse.

2. Formål

Formålet med årsrapporten er at give kommunalbestyrelsen indsigt i kommunens arbejde med informationssikkerhed og databeskyttelse for det forgangne år.

Årsrapporten 2023 følger derfor op på fokusområder i den tilsvarende rapport for 2022 med anbefalinger til følgende år.

3. Metode

Årsrapporten beskriver generelt og overordnet kommunens status for arbejdet med informationssikkerhed og databeskyttelse. Indholdet bygger på databeskyttelsesrådgiverens observationer og kontroller samt organisations notater, statistikker og analyser af de gennemførte indsatser det seneste år.

4. Databeskyttelsesrådgiveren i Norddjurs Kommune

Databeskyttelsesrådgiveren i Norddjurs Kommune er lederen for IT og Digitalisering. Det daglige arbejde med databeskyttelse varetages af en fuldtids databeskyttelseskoordinator og suppleres af kommunens informationssikkerhedskoordinator og contract manager.

5. Det forgangne år – 2023

Afsnittet giver indsigt i kommunens arbejde med informationssikkerhed og persondatabeskyttelse på prioriterede områder.

5.1 Status på anbefalinger til fokusområder i det forgangne år

I dette afsnit samles der op på databeskyttelsesrådgiverens liste af anbefalinger fra sidste års rapport.

5.1.1 Sletning og arkivering

Som følge af det skriftlige og fysiske tilsyn i 2022 har der i det forgangne år været fokus på sletning og arkivering af data på tværs af kommunens fagområder.

Arbejdet med risikostyring, herunder blandt andet gennem risikovurderinger af IT-systemer og behandlingsaktiviteter samt indgåelse af databehandleraftaler, har medført et øget fokus på sletning af borgernes data efter endt behandling.

Et eksempel på arbejdet med sletning og arkivering er i Skole- og Dagtilbud, hvor der har været nedsat en arbejdsgruppe, der blandt andet har arbejdet med mulighederne for sletning i fagsystemer samt arkivering via journaliseringssystemer.

5.1.2 Afprøvning af beredskabsplan

Én af anbefalingerne fra 2022 var at afprøve beredskabsplanen. Det blev gennemført ved KL og DCIS Sunds beredskabsøvelse 2023, som alle danske kommuner var inviteret til at deltage i.

Beredskabsøvelsen gav anledning til enkelte tilretninger i IT-beredskabsplanen, herunder men ikke begrænset til:

- Printe beredskabsplanen, så den ikke kun findes digitalt – herunder også Norddjurs Kommunes overordnede beredskabsplan
- Procedure for ajourføring af beredskabsplanen
- Behovet for en FM-radio
- Koblinger mellem IT-afdelingen og Krisestaben

Dermed medførte beredskabsøvelsen flere opmærksomhedspunkter, som it-afdelingen kan tage med i arbejdet med den videre udvikling af IT-beredskabsplanen.

5.1.3 Decentrale kontaktpersoner

I 2023 har cheferne for de enkelte fagområder udpeget lokale kontaktpersoner for Norddjurs Kommunes informationssikkerhedsteam. Formålet med disse kontaktpersoner er at have et direkte kontaktpunkt for informationssikkerhedsteamet ud i fagområderne. Kontaktpersoner skal bidrage til at skabe sammenhængen mellem de centrale og decentrale dele af organisationen. Roller, ansvar og forventninger til kontaktpersoner er drøftet og afstemt i Informationssikkerhedsudvalget.

5.2 Andre fokusområder i det forgangne år

En stor del af 2023 har været fokuseret omkring optimering af de systemer, der bruges i arbejdet med databeskyttelse og informationssikkerhed samt Datatilsynets fokusområder. Tre af disse fokusområder lå til baggrund for det skriftlige og fysiske tilsyn i fagområderne i 2023.

5.2.1 TV-overvågning

Datatilsynet har tidligere ført tilsyn med blandt andet offentlige myndigheders behandling af personoplysninger i forbindelse med TV-overvågning. Informationssikkerhedsteamet satte i 2023 derfor fokus på Norddjurs Kommunes TV-overvågning.

Der er blevet skabt et overblik over kommunens TV-overvågning, og der er udarbejdet en procedure for bestilling af QR-koder, der sættes op ved alle kommunens kameraer. QR-koderne linker borgere og medarbejdere direkte til oplysningspligten på kommunens hjemmeside, Norddjurs.dk.

5.2.2 Oplysningspligt og behandlingshjemmel

Det er ikke kun i arbejdet med TV-overvågning, at der har der været fokus på oplysningspligt og behandlingshjemmel.

Det skriftlige tilsyn blev i foråret 2023 sendt ud til chefer for alle fagområderne, og her blev der blandt andet spurgt ind til oplysningspligt og behandlingshjemmel i forbindelse med områdernes kerneopgaver. Disse besvarelser blev uddybet yderligere under det fysiske tilsyn i efteråret 2023, hvor Sundhed og Omsorg, Kultur og Udvikling samt Vej og Ejendom fik besøg af Informationssikkerhedsteamet. Her blev der skabt rum for dybdegående samtaler omkring oplysningspligt blandt andet ved modtagelse af skriftlige henvendelser, og i hvilke tilfælde, samtykke kan benyttes som behandlingshjemmel i en offentlig myndighed.

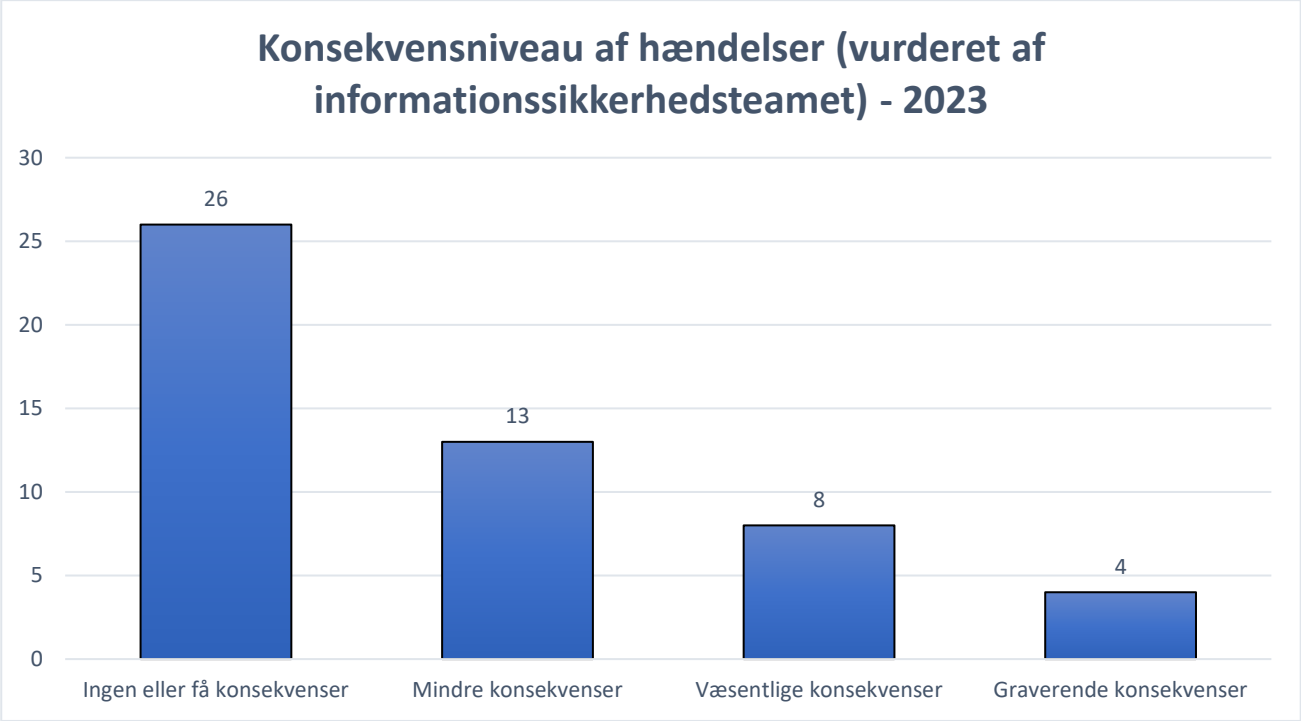
5.3 Sikkerhedshændelser og -brud

Lovgivningen forpligter Norddjurs Kommune at registrere alle sikkerhedsbrud og -hændelser. Hvis disse indebærer risici for de registreredes rettigheder, så skal de desuden anmeldes til Datatilsynet. Vurderer kommunen derudover, at bruddet indebærer store risici for de registreredes rettigheder, så skal kommunen endvidere underrette den registrerede om bruddet.

Norddjurs Kommune har i 2023 registreret 45 persondatabrud, mens der er blevet indberettet 58 sikkerhedshændelser. I 34 ud af de 45 persondatabrud har der været tale om borgeres data, mens medarbejderes data også har været berørt i 10 af sagerne.

De mest hyppige personoplysninger, der har indgået i brud på persondatasikkerheden i det forgangne år, har været navn, helbredsoplysninger, fødselsdato og personnummer.

Som grafen nedenfor viser, så har størstedelen af bruddene på persondatasikkerheden medført ingen, små eller mindre konsekvenser for de registrerede.



6. Anbefalinger til fokusområder i 2024

I det følgende beskrives både anbefalinger fra Norddjurs Kommunes databeskyttelsesrådgiver samt relevante fokusområder fra Datatilsynet i 2024.

6.1 Datatilsynets anbefalinger til fokusområder i 2024

Anbefalingerne i dette afsnit er baseret på Datatilsynets særlige fokusområder for tilsynsaktiviteter i 2024.

6.1.1 Brug af kunstig intelligens og automatisering

Kunstig intelligens og automatisering har de seneste år – og vil fortsat – fylde meget i det offentlige, og her er Norddjurs Kommune ingen undtagelse, da vi flere steder i kommunen benytter os af disse nye teknologier.

Disse indebærer dog særlige risici for de borgere, hvis oplysninger bliver behandlet som led i udvikling eller brug af løsningerne. Datatilsynet vil derfor i 2024 fortsat fokusere på kunstig intelligens og automatisering blandt andet gennem tilsyn med offentlige myndigheder.

6.1.2 Rettighedsstyring og forebyggelse af misbrug af adgang til personoplysninger

Rettighedsstyring har de seneste år været et fokusområde for både informationssikkerhedsteamet og IT-afdelingen. Nu har Datatilsynet også sat sig for at føre tilsyn med, om de nødvendige tekniske og organisatoriske sikkerhedsforanstaltninger er implementeret i blandt andet de danske kommuner for at sikre, at borgernes personoplysninger ikke bliver gjort tilgængelige for uvedkommende ved for eksempel misbrug af adgangsrettigheder.

Der har de seneste år været flere eksempler på, hvordan mangelfuld rettighedsstyring har forøget risikoen for misbrug af borgernes personoplysninger, blandt andet fordi medarbejdere uberettiget tilgår personoplysninger af enten nysgerrighed eller med ondsindede intentioner. Systematisk rettighedsstyring, udbredte procedurer samt awareness er dermed centrale redskaber for sikring af data i Norddjurs Kommune.

6.1.3 Grundlæggende behandlingssikkerhed hos kommuner og regioner

Siden 2020 har Datatilsynet ført såkaldte modenhedstilsyn med fokus på grundlæggende behandlingssikkerhed hos både kommuner og regioner. Nogle af de områder, som Datatilsynet vil fokusere på i forbindelse med grundlæggende behandlingssikkerhed i kommunerne, er blandt andet kryptering af bærbare computere, scanningsværktøjer og udarbejdelse af konsekvensanalyser.

6.2 Databeskyttelsesrådgiverens anbefalinger til fokusområder i 2024

Anbefalingerne i dette afsnit er baseret på databeskyttelsesrådgiverens egne observationer og vurderinger af konkrete behov i Norddjurs Kommune. De nedenstående fokusområder taler desuden direkte ind i Datatilsynets interesse i at undersøge den grundlæggende behandlingssikkerhed hos offentlige myndigheder.

6.2.1 Ajourføring af fortegnelser

Databeskyttelsesforordningen stiller krav om, at alle dataansvarlige fører interne fortegnelser over alle behandlingsaktiviteter, der indeholder personoplysninger. Dette er også en væsentlig del af den grundlæggende behandlingssikkerhed hos offentlige myndigheder. Hos Norddjurs Kommune har vi allerede udarbejdet fortegnelser over behandlingsaktiviteter inden for alle fagområderne. Men for at leve op til kravene om databeskyttelse, skal disse revideres årligt. Dette blandt andet for at skabe overblik over, hvilke oplysninger, vi behandler i vores IT-systemer. Databeskyttelsesrådgiveren anbefaler derfor, at alle fagområder ajourfører deres fortegnelser i 2024.

6.2.2 Udarbejdelse og ajourføring af risikovurderinger og konsekvensanalyser

De seneste år er vi kommet langt med risikostyring inden for IT-systemer og behandlingsaktiviteter, men for at kunne opretholde et højt sikkerhedsniveau, så er det vigtigt, at der fortsat er fokus på både udarbejdelse

og ajourføring af risikovurderinger for anvendte IT-systemer i kommunen samt udarbejdelse af konsekvensanalyser for systemer, hvor behandling af personoplysninger kan medføre høj konsekvens for de registrerede.

6.2.3 Leverandørstyring

For at sikre det rette sikkerhedsniveau inden for behandlingen af personoplysninger, så er det vigtigt, at vi kontrollerer, hvordan blandt andet leverandører af vores IT-systemer lever op til relevante sikkerhedskrav. Derfor er det en anbefaling for 2024, at der udover indgåelse af databehandleraftaler også kommer fokus på blandt andet revisionserklæringer for kommunens leverandører.

7. Konkluderende bemærkninger

Formålet med statusrapporten er at give svar på:

- Hvordan er Norddjurs kommunes tilstand i forhold til databeskyttelse i 2023?
- Hvilken udvikling har der været fra 2022 til 2023?
- Hvilke fokusområder anbefaler databeskyttelsesrådgiveren at arbejde videre med i 2024?

Arbejdet med databeskyttelse og informationssikkerhed er grundlæggende implementeret efter både databeskyttelsesforordningen, ISO 27001 samt NSIS (National Standard for Identiteters Sikringsniveauer). Dermed handler det daglige arbejde om at vedligeholde og videreudvikle sikkerheden omkring både Norddjurs Kommunes IT-systemer, fysiske rammer og arbejdsgange.

For at sikre opretholdelse af sikkerhedsniveauet på tværs af organisationen, så er det vigtigt, at Informationssikkerhedsteamet har et godt samarbejde med fagområderne. Her behandles store mængder personoplysninger, og derfor bør det generelle fokus i 2024 være at fremme arbejdet med databeskyttelse og informationssikkerhed, der hvor borgernes og medarbejdernes personoplysninger primært behandles.