norddjurs kommune

DATABESKYTTELSES-RÅDGIVERENS ÅRSRAPPORT 2021

maj 2022

Indholdsfortegnelse

1. Indledning

Rapportering af arbejdet med informationssikkerhed og databeskyttelse foregår årligt og udformes som databeskyttelsesrådgiverens årsrapport.

Covid-19 har fortsat betydet meget i det forgangne år med hjemmearbejde for mange faggrupper. Det har til tider været anderledes med mange nye arbejdssteder og arbejdsgange. I Norddjurs Kommune har vi kæmpet os igennem den svære tid, fået det bedste ud af omstændighederne og lært en masse nyt.

Vi blev sidste år introduceret til Schrems II-sagen, der har betydet, at vi i Norddjurs Kommune ligesom i landets øvrige kommuner fortsat har haft stor fokus på, at data ikke direkte overføres til usikre tredjelande som fx USA.

Norddjurs Kommune gennemførte i 2021 et skriftlig tilsyn fra Datatilsynet. Vi fik en rapport i slutningen af året, hvor det var muligt at se kommunens besvarelse og sammenligning til andre offentlige myndigheders besvarelser. I rapporten fremgik anbefalinger i form af fokuspunkter, som kommunen kan arbejde videre med.

2. Formål

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

Årsrapporten 2021 følger op på fokusområderne i den tilsvarende rapport for 2020 med anbefalinger for følgende år.

3. Metode

Årsrapporten beskriver generelt og overordnet kommunens status for arbejdet med informationssikkerhed og databeskyttelse. Indholdet bygger på databeskyttelsesrådgivers observationer og kontroller samt organisationens notater, statistikker og analyser af de gennemførte indsatser.

4. Databeskyttelsesrådgiveren i Norddjurs Kommune

Databeskyttelsesrådgiveren for årsrapporten 2021 er afdelingslederen for IT og Digitalisering. Det blev han i februar måned 2021 efter den tidligere databeskyttelsesrådgiver fik ansættelse i en anden kommune. Den nuværende informationssikkerhedskoordinator, der blev fastansat i sommeren 2021, har været tæt inde over databeskyttelsesrådgiveropgaverne. Organiseringen med adskilte roller som databeskyttelsesrådgiver og informationssikkerhedskoordinator har været et opmærksomhedspunkt siden 2019.

Det nære samarbejde mellem Norddjurs, Syddjurs og Favrskov Kommune er i fortsat vækst. Kommunerne finder flere og flere opgaver og projekter, hvor det giver mening at samarbejde. Eksempelvis vil arbejdet med indgåelse af databehandleraftaler og tilsyn med databehandlere fremadrettet ske i tæt samarbejde med Syddjurs Kommune.

5. Hjemmearbejde

Den fortsatte nedlukning af samfundet har været med til, at vi som organisation har vænnet os til at få hverdagen til at hænge sammen på andre måder end tidligere. Covid-19 har gjort det vanskeligt med fysisk undervisning, hvilket har udviklet vores anvendelse af digitale redskaber til at udføre awareness inden for informationssikkerhed og databeskyttelse. Med forøgelsen af hjemmearbejde har det været nødvendigt i højere grad end tidligere at fokusere indsatsen og opmærksomheden på at håndtere forskellige former for cyberangreb.

6. Det forgangne år – 2021

Dette afsnit giver indblik i Norddjurs Kommunes arbejde med både persondatabeskyttelse

og informationssikkerhed, samt de justeringer der i løbet af året er foretaget i den overordnede organisering af området.

6.1: Justering af organiseringen mv.

Norddjurs Kommune har i 2021 sikret, at de overordnede styringsdokumenter er behandlet og godkendt i Direktionen. Disse styringsdokumenter består af tværgående retningslinjer for informationssikkerhed, strategi for informationssikkerhed og databeskyttelses awareness samt risikometode.

Informationssikkerhedsudvalget, der er nedsat af Direktionen, har fortsat kvartals møder. Der har desværre været relativ stor udskiftning blandt udvalgets medlemmer, men kontinuiteten i udvalgets arbejde er sikret gennem dokumentation ved dagsordner, bilag og referater.

IT-sikkerhedsgruppen har fået ny formand efter IT-afdelingen har fået ny afdelingsleder, og er fortsat tæt koblet til Informationssikkerhedsudvalget. Gruppen har særligt fokus på teknisk sikkerhed, cybersikkerhed og diverse trusler fra omverden.

Databeskyttelsesteamet er blevet styrket siden seneste årsrapport, idet afdelingslederen for IT og Digitalisering overtog rollen som databeskyttelsesrådgiver samtidig med, at informationssikkerhedskoordinatoren blev fastansat i sommeren 2021. Der blev i slutningen af året endvidere ansat en projektleder i afdelingen, som delvis understøtter arbejdet med informationssikkerhed og databeskyttelse.

6.2: Efterlevelse af databeskyttelseslovgivningen

Dette afsnit besvarer delformålet om, hvordan Norddjurs Kommune efterlever databeskyttelseslovgivningen. Dokumentation er en vigtig del af arbejdet med databeskyttelse.

6.2.1: Opfølgning på artikler fra årsrapport 2020

6.2.1: Kommunens håndtering af databehandleraftaler og tilsyn

Norddjurs Kommune har vedligeholdt et overblik over databehandleraftaler for IT-systemerne. Tilsynene med databehandlerne blev foretaget i samarbejde med nabokommunerne Syddjurs og Favrskov Kommune. Ud af 144 IT-systemer er der fortaget tilsyn på 61 IT-systemer. De resterende er primært begrundet i manglende indhentning af revisionserklæring. Dette er en stigning på 3 % fra foregående år. Norddjurs bør fortsat have fokus på kommunens håndtering af databehandleraftaler og tilsyn. Samarbejdet med Syddjurs Kommune og Det Fælles KL-Sekretariat er eksempler på tiltag, der vil øge antallet af tilsyn i 2022 betragteligt.

Der har i 2021 været stor fokus på overførsel til tredjelande i forlængelse af Shrems-II dommen i 2020. Kommunerne har afventet, at der kom klare retningslinjer fra KL eller Datatilsynet om især brug af amerikanskejede cloudløsninger, hvor data opbevares i EU.

Der er ved udgangen af 2021 ikke kommet en klar vejledning til, hvordan disse skal behandles. Der er derfor opmærksomhed på, hvilke afgørelser der kommer på dette område i 2022.

6.2.2: Fortegnelser over behandlingsaktiviteter

Artikel 30 i databeskyttelsesforordningen beskriver, at Norddjurs Kommune skal føre fortegnelser over de behandlinger kommunen foretager. Fortegnelserne er lister, som blandt andet indeholder oplysninger om formålet med en behandling, hvilke personoplysninger der indgår og om oplysningerne bliver overført til tredjelande.

Norddjurs Kommune reviderede fortegnelserne i november og december 2021. Ændringerne har været få, idet typen af behandling af personoplysninger i en kommune ikke ændrer sig væsentlige fra år til år.

For at efterleve en revideret vejledning fra Datatilsynet, så påbegynder Norddjurs Kommune arbejdet med fortegnelserne på ny i 2022 baseret på materiale udarbejdet af KL.

6.2.3: Risikovurderinger og konsekvensanalyser

Risikostyring er et væsentligt element i at forebygge at både systemer og mennesker ikke fejlagtigt publicerer, ændrer eller mister adgang til fortrolige oplysninger.

Norddjurs Kommunes tilgang til udførelsen af risikovurderingerne er, at de kritiske behandlinger bliver prioriteret først. Det betyder i praksis, at de store fagsystemer med store mængder af fortrolige og følsomme personoplysninger er prioriteret.

I 2021 foretog kommunen 21 risikovurderinger mod 6 risikovurderinger i 2020.

bruddet indebærer store risici for de registreredes rettigheder, så skal kommunen underrette den registrerede om bruddet.

I 2021 har kommunen registreret 50 sikkerhedshændelser, hvoraf 43 var brud på persondatasikkerheden. Til sammenligning var tallene i 2019 20 sikkerhedshændelser, hvoraf 15 var brud på persondatasikkerheden og i 2020 55 sikkerhedshændelser, hvoraf 45 var brud på persondatasikkerheden. Det er et marginalt fald fra sidste år, som det er vanskeligt endegyldigt at konkludere årsagen til.

Sikkerhedshændelserne omhandler flere typer af persongrupper (registrerede). De registrerede fordeler sig primært på voksne borgere (32 sager) og mindreårige borgere (18 sager), men der findes også enkelte sager med medarbejdere (se diagram 1).

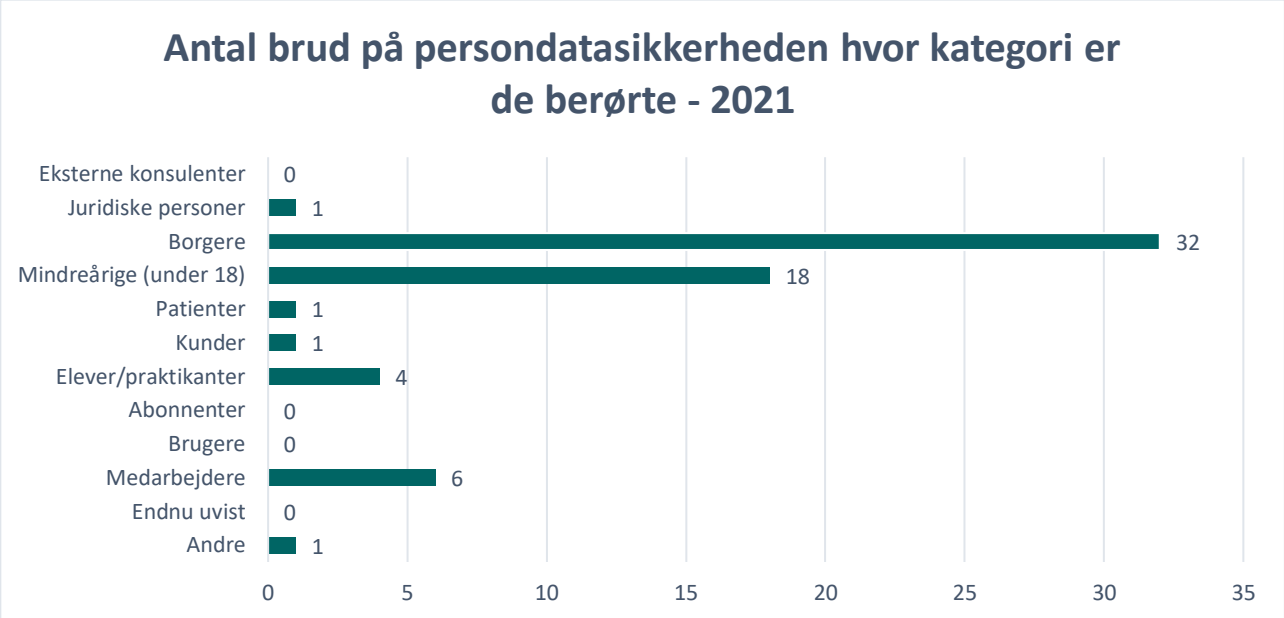

Diagram 1 Antal brud på persondatasikkerheden, hvor en bestemt kategori af registrerede har indgået. 'Endnu uvist' dækker en hændelse, hvor der ikke blev konstateret om der var sket et konkret brud på persondatasikkerheden

6.2.4: Sikkerhedshændelser og sikkerhedsbrud

Lovgivningen forpligter Norddjurs Kommune at registrere alle sikkerhedsbrud. Hvis disse brud indebærer risici for de registreredes rettigheder, så skal de desuden anmeldes til Datatilsynet. Vurderer kommunen desuden, at

De mest hyppige oplysninger, som har indgået i et brud på persondatasikkerheden i 2021, har været registreredes navne, personnumre, fødselsdatoer (som også indgår i personnummeret) og andre typer personoplysninger, som fx kan være billeder, ferieforhold, forældremyndighed eller lånerstatus på biblioteker.

6.2.5: Awarenesstiltag

Der er i løbet af 2021 udført følgende awarenesstiltag.

1. Årlig recertificering ved brug af kommunens e-læringskursus om databeskyttelse.
2. Banner på intranettet for at synliggøre og illustrere hvad der anses som værende sikkerhedsbrud.
3. Banner der viser årsager og størrelser af bøder udstedt af Datatilsynet.

Intranettet blev taget i anvendelse i 2020 og indeholder alt relevant materiale vedrørende databeskyttelse og informationssikkerhed. Nyt materiale tilføjes løbende.

Årets afsluttende awarenesstiltag var at genudsende kommunens e-læringskursus om databeskyttelse, hvor kursets indhold var tilpasset brugernes behov på forskellige niveauer.

6.2.6: Kontrol og opfølgning på arbejdet

Dette afsnit skal både ses som en statusbeskrivelse af tilsynsarbejdet, men det har også et fremadrettet perspektiv.

Ved årsskiftet 2020/2021 blev det første fysiske tilsyn udført i Borgerservice. Tilsynet var både konkret, men også et pilotforsøg på fysiske tilsyn fremover.

Pilotforsøget forventes at blive opfulgt af et skriftligt tilsyn, der udsendes til samtlige systemejere. De skriftlige tilsyn følges op på med fysisk tilsyn for særligt udvalgte. Dette forventes udført i løbet af 2022.

7. Databeskyttelsesrådgiverens anbefalinger til fokusområder i 2022

I det følgende beskrives databeskyttelsesrådgiverens anbefalinger til fokusområder for Norddjurs Kommune i 2022. Anbefalingerne er i år baseret på Datatilsynets anbefalinger fra rapporten fra det skriftlige tilsyn og udvalgte punkter taget fra Datatilsynets særlige fokusområder for tilsynsaktiviteter i 2022.

1. Skab overblik over behandlingsaktiviteter og de risici for de registrerede, der er forbundet med behandlingsaktiviteterne og etablér strukturerede arbejdsgange til regelmæssigt at evaluere tiltag inden for databeskyttelse og informationssikkerhed.
2. Evaluér beskyttelsen af adgange til systemer og databaser, hvor der opbevares og behandles personoplysninger, med henblik på at sikre effektive foranstaltninger.
3. Afprøv om foranstaltninger, herunder beredskab, som udgør grundlæggende sikkerhed, er virkningsfulde og effektive til at reetablere drift under angreb og til at håndtere hændelser.
4. Norddjurs Kommune skal som dataansvarlig sikre, at personoplysninger der sendes udenfor EØS-landene, overgår til de fornyede standardkontrakter (SSC) inden udgangen af 2022.
5. Norddjurs Kommune har i 2020 haft fokus på at lave et overblik over tv-overvågning i kommunen, dette bør der følges op på jævnfør oplysningspligten.

Nedenfor bliver de fem fokuspunkter gennemgået.

7.1: Skab overblik over behandlingsaktiviteter

Databeskyttelsesforordningen forpligter Norddjurs Kommune til at føre fortegnelser over behandlingsaktiviteterne. Dette arbejde er hidtil udført med KL's skabelon. Datatilsynet har siden hen revideret deres forventninger til, hvordan arbejdet med fortegnelser bør udføres. For at efterleve dette har KL udarbejdet nyt materiale.

I slutningen af 2021 investerede kommunen i et nyt it-system, der har til formål at samle store dele af arbejdet med databeskyttelse og informationssikkerhed i et samlet it-system. Dette gælder også for arbejdet med fortegnelser, der skal ajourføres hvert år.

Databeskyttelsesrådgiveren anbefaler på den baggrund, at Norddjurs Kommune overgår til det nye materiale og behandlingsaktiviteter udarbejdet af KL.

7.2: Evaluér beskyttelsen af adgange til systemer og databaser

Norddjurs Kommune skal sikre, at det kun er autoriserede personer, der har adgang til personoplysninger. Det udføres ved at etablere et systematisk overblik, hvor den enkelte medarbejder kun har adgang til personoplysninger der er arbejdsbetinget.

Databeskyttelsesrådgiveren anbefaler på den baggrund, at Norddurs Kommune udfører skriftligt og derefter fysisk tilsyn for at efterprøve adgangen til it-systemer og databaser i Norddjurs Kommune.

7.3: Afprøv sikkerheden

Norddjurs Kommune har etableret en række foranstaltninger for at sikre, at sikkerhedsniveauet i kommunen forbliver på et passende niveau.

Databeskyttelsesrådgiveren anbefaler på den baggrund, at Norddjurs Kommune afprøver sikkerheden ved at simulere nedbrud under kontrollerede forhold.

7.4: Deadline for indgåelse af standardkontrakt

Europa-Kommissionen har den 4. juli 2021 vedtaget et sæt nye standardkontrakter.

- Overførsel af personoplysninger fra en dataansvarlig inden for EØS til en dataansvarlig uden for EØS
- Overførsel af personoplysninger fra en dataansvarlig inden for EØS til en databehandler uden for EØS
- Overførsel af personoplysninger fra en databehandler inden for EØS til en databehandler uden for EØS
- Overførsel af personoplysninger fra en databehandler inden for EØS til en dataansvarlig uden for EØS (som ikke er omfattet af databeskyttelsesforordningens regler efter artikel 3, stk. 2)

Ovenstående scenarier beskriver, hvordan de nye standardkontrakter bør tages i brug. Deadline for, at alle aftaler skal være overgået til de nye standardkontrakter er den 27. december 2022.

Databeskyttelsesrådgiveren anbefaler på den baggrund, at Norddjurs Kommune gennemgår eksisterende aftaler og sikrer, at nye aftaler indgås efter de nye regler.

7.5: Oplysningspligt med tv-overvågning

Norddjurs Kommune lavede i 2020 et overblik over hvor der eksisterer tv-overvågning i kommunen.

Databeskyttelsesrådgiveren anbefaler på den baggrund, at Norddjurs Kommune ajourfører overblikket over tv-overvågning og sikrer oplysningspligten i samme forbindelse.

8. Konkluderende bemærkninger

Formålet med statusrapporten er at give svar på:

- Hvordan er Norddjurs kommunes tilstand i forhold til databeskyttelse i 2021?
- Hvilken udvikling har der været fra 2020 til 2021?
- Hvilke fokusområder anbefaler databeskyttelsesrådgiveren at arbejde med i 2022?

Norddjurs Kommune har i 2021 afsluttet en periode, så databeskyttelsesforordningen ikke længere er under implementering, men databeskyttelse er en naturlig del af driftsopgaverne.

Der er fortsat plads til udvikling af databeskyttelsesområdet, ligesom der er områder inden for databeskyttelse, som bør have særlig fokus i de kommende år. Der vil formentligt altid være et udviklingspotentiale, da databeskyttelse hele tiden udvikler sig i forhold til det omkringliggende samfund. Et eksempel på dette er krigen i Ukraine, der

har givet et fornyet fokus på spionage og cyberangreb.

Overordnet er der i Norddjurs Kommune styr på rammerne for databeskyttelse. Styringsdokumenter er udarbejdet, godkendt og implementeret. Og der er indført et årshjul med de opgaver, der skal varetages i forhold til databeskyttelse.

I forhold til udviklingen fra 2020 til 2021, så har der været udfordringer både med udskiftning af centrale medarbejdere og i forhold til Covid-19, som har besværliggjort samarbejdet med fagområderne. Der har dog stadig været en fornuftig udvikling på hele området.

I forhold til risikostyring, så er antallet af gennemførte risikovurderinger steget med over 400% fra 2020 til 2021. Der pågår dog stadig et stort arbejde i at få risikovurderet samtlige persondatabærende it-systemer.

På samme måde er tilsynet med databehandlere udviklet i 2021, men som det fremgår af opgørelsen i afsnit 6.2.1, så er der også her plads til udvikling. Der er derfor iværksat tiltag, der skal løfte andelen af tilsyn i 2022, blandt andet ved indgåelse af samarbejde med Syddjurs Kommune og tilslutning til et fælles KL-sekretariat, som skal løfte opgaven på de store fælles it-systemer i kommunerne.

Det er databeskyttelsesrådgiverens anbefaling, at der i 2022 er ekstra fokus på følgende områder:

- Skab overblik over behandlingsaktiviteter
- Adgangsstyring til data og it-systemer
- Afprøv sikkerhedsniveauet
- Gennemgå eksisterende aftaler og forny standardaftaler
- Oplysningspligt ved kameraovervågning
- Cybersikkerhed