norddjurs kommune

DATABESKYTTELSES-RÅDGIVERENS **ÅRSRAPPORT 2020**

April 2021

Indholdsfortegnelse

1. Indledning

Kommunalbestyrelsen behandler og godkender én gang i hver byrådsperiode kommunens informationssikkerhedspolitik. Rapportering af arbejdet med informationssikkerhed og persondatabeskyttelse sker én gang årligt i form af databeskyttelsesrådgivers årsrapport (dette dokument).

Kommunalbestyrelsen besluttede på mødet den 25. august 2020 en ny informationssikkerhedspolitik for Norddjurs Kommune. Politikken med de tilhørende styringsdokumenter er nu rammesættende for alle vejledninger og retningslinjer, der udgør grundlaget for arbejdet med informationssikkerhed og databeskyttelse i organisationen.

To emner har fyldt meget i 2020. For det første har Covid-19 med øget anvendelse af hjemmearbejde betydet mange nye arbejdsgange og private it-installationer har haft afsmittende virkning på blandt andet persondataområdet og den igangværende indsats med databehandlerkulturen i Norddjurs. For det andet afsagde EU-domstolen i sommeren 2020 en markant afgørelse i forbindelse med Schrems II-sagen. Sagen handler om overførsel af personoplysninger til lande uden for EU og specielt USA, men også data i datacentre beliggende i EU, hvor leverandøren er hjemhørende uden for EU.

På trods af Covid-19 har 2020 været et år, hvor Norddjurs Kommune har taget mange gode skridt i bestræbelserne på at få EU-persondataforordningen til at fungere tilfredsstillende i kommunal sammenhæng.

2. Formål

Formålet med databeskyttelsesrådgiverens årsrapport er at give kommunalbestyrelsen indsigt i kommunens status med databeskyttelsesarbejdet for det forgangne år.

Årsrapporten 2020 følger op på fokusområderne i den tilsvarende rapport for 2019 med anbefalinger for følgende år. På samme måde vil denne rapport indeholde anbefalinger til fokusområder for 2021.

3. Metode

Årsrapporten beskriver generelt og overordnet kommunens status for databeskyttelsesarbejdet.

Indholdet bygger på databeskyttelsesrådgivers observationer og kontroller samt organisationens notater, statistikker og analyser af de gennemførte indsatser.

4. Databeskyttelsesrådgiveren i Norddjurs Kommune

Databeskyttelsesrådgiveren for rapportens periode 2020 blev ansat i efteråret 2019 og valgte fra februar 2021 at søge nye udfordringer i en anden kommune. Rollen som databeskyttelsesrådgiver er efterfølgende håndteret internt i organisationen. Samtidig er rollerne som databeskyttelsesrådgiver og informationssikkerhedskoordinator blevet adskilt. Dette var et af opmærksomhedspunkterne i rapporten for 2019.

I løbet af 2020 har samarbejdet mellem databeskyttelsesrådgiver og organisationen udviklet sig i en positiv retning. Ledere og medarbejdere er i stigende grad begyndt at kontakte og anvende de kompetencer, som databeskyttelsesrådgiveren besidder. Det har alt i alt været med til at indfri forventningerne til en sund databehandlingskultur.

Partnerskabet med Århus Universitet har desuden givet inspiration til at studerende har været i studiepraktik i Norddjurs.

Det nære samarbejde med Syddjurs og Favrskov Kommuner på IT- og digitaliseringsområdet har givet anledning til et godt netværk mellem kommunernes centrale medarbejdere på dette område. Erfaringsudveksling, deling af kompetencer og løsning af opgaver på tværs, er blevet øget i perioden.

5. Covid-19 pandemien og databeskyttelsesarbejdet

Nedlukningen som følge af udbruddet af Covid-19 i marts 2020 vanskeliggjorde fysisk undervisning af medarbejderne. Men ligesom på mange andre områder blev de digitale platforme taget i anvendelse. På den ene side var det en udfordring i arbejdet med kompetenceudvikling, men på den anden side gav det også anledning til særlig fokus på datasikkerhed, når arbejdspladsen var uden for de vante rammer. Spørgsmål om hvor og hvordan persondata opbevares, blev aktuelt på andre måder.

6. Det forgangne år – 2020

Dette afsnit giver et 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.

Den nye informationssikkerhedspolitik, der blev besluttet i august 2020, gav anledning til nye og supplerende styringsdokumenter, der løbende er behandlet og godkendt i Direktionen. Et af disse dokumenter er Norddjurs Kommunes informationssikkerhedsstrategi, der beskriver mål for både informationssikkerheds- og databeskyttelsesarbejdet de kommende år. Strategien indeholder desuden en governance struktur der fordeler roller og ansvar i organisationen.

Direktionen har nedsat et informationssikkerhedsudvalg til at understøtte den overordnede tværgående indsats på området. Formanden for Informationssikkerhedsudvalget er koblingen til Direktionen og har dialogen med direktørerne om emner der er relevante for Direktionen.

Informationssikkerhedsudvalget fik justeret kommissoriet i maj måned 2020, hvor udvalget blev udvidet i bestræbelserne på at dække hele organisationen. Udvalget er de seneste år blevet godt konsolideret og varetager de relevante tværgående strategiske overvejelser i forhold til den gode databehandlingskultur og persondatasikkerhed.

IT-sikkerhedsgruppen (teknisk sikkerhed) er i 2020 blevet omstruktureret og har en tæt sammenhæng til Informationssikkerhedsudvalget. Gruppen har særlig fokus på cybersikkerhed og de forskellige trusler fra omverdenen.

Organisationen er nået langt med forrige års anbefaling om organisering og ansvar i informationssikkerhedsarbejdet, og indsatserne fortsætter i kraft af undervisning og awareness-kampagner.

6.2: Efterlevelse af databeskyttelseslovgivningen

Dette afsnit besvarer delformålet om, hvordan Norddjurs Kommune efterlever databeskyttelseslovgivningen. Artikel 5 i forordningen beskriver principperne for behandling af personoplysninger. Herunder findes artikel 5, stk. 2., som ligeledes påbyder dataansvarlige at kunne påvise deres overholdelse af databeskyttelsesprincipperne. Dokumentation er en vigtig del af arbejdet med databeskyttelse.

Afsnit 6.2 er yderligere opdelt i to. Først vil der være en opfølgning på artiklerne, som var i fokus i årsrapporten 2019. Dernæst vil der blive introduceret nye artikler, som sættes i fokus i 2020. Intentionen er, at der primært følges op på de nye artikler i næstkommende årsrapport, medmindre andet vurderes nødvendigt.

Konkret betyder det, at der vil være en opfølgning på artikel 13 og 14 om oplysningspligt, artikel 28 om databehandlere, artikel 30 om fortegnelser over behandlingsaktiviteter, artikel 32 om behandlingssikkerhed, artikel 33 om anmeldelser af brud på persondatasikkerheden, artikel 35 om konsekvensanalyse og artikel 39 hvori indgår databeskyttelsesrådgivers kontrol af undervisning og opmærksomhedskampagner for kommunens personale.

I sidste delafsnit vil følgende artikler blive belyst. Artikel 5 om principperne for behandling af personoplysninger, artikel 6 og 9 om lovlig behandling af henholdsvis personoplysninger og særlige kategorier af personoplysninger og artikel 12 samt 15-21 om persondatarettighederne. Desuden vil afsnittet rumme et underafsnit omkring Norddjurs Kommunes TV-overvågning, som både databeskyttelsesforordningen og TV-overvågningsloven regulerer.

6.2.1: Opfølgning på artikler fra årsrapport 2019

6.2.1.1: Oplysningspligt

Når Norddjurs Kommune indsamler personoplysninger fra en registreret, eller modtager dem fra en tredjepart, skal den registrerede blandt andet orienteres om, hvad oplysningerne anvendes til. Undtagelsen for denne orientering er, hvis den registrerede er bekendt med behandlingen, eller hvis behandlingen jævnfør anden lov er fortrolig.

Kommunen har i 2020 fortsat ad-hoc med at kvalificere orienteringerne, som afgives i forbindelse med indsamling af de registreredes oplysninger. Der er blandt andet blevet udarbejdet en procedure samt skabeloner til iagttagelsen af oplysningspligten (se afsnit 6.2.2.3 for reference til proceduren), for at standardisere og hjælpe forvaltningen med at efterleve lovgivningen.

I forbindelse med en gennemgang af Norddjurs Kommunes blanketter, har Norddjurs Kommune i øvrigt afgivet notat til Kommunernes Landsforening (KL), grundet mangler ift. informationsniveauet i blanketterne. KLs blanketter anvendes når borgere for eksempel søger ydelser i kommunen. Disse blanketter skal afgive den korrekte orientering til de registrerede, hvad end blanketterne anvendes i fysisk form eller digitalt på Borger.dk. Norddjurs Kommunes bidrag til KL bestod blandt andet af, hvilke elementer af blanketterne kunne kvalificeres yderligere, herunder også hvordan KL fortsat kunne arbejde med blanketterne.

Der har desuden været et fokus på, hvilke cookies[1] kommunen påbyder besøgende på kommunens hjemmeside, hertil hvordan de besøgende orienteres om diverse cookies, og hvilke de kan fravælge når de besøger hjemmesiden.

Det anbefales fortsat, at Norddjurs Kommune arbejder med at kvalificere sin iagttagelse af oplysningspligten. Dette kan blandt andet ske med udgangspunkt i kommunens fortegnelser over behandlingsaktiviteter (se afsnit 6.2.1.3).

6.2.1.2: Kommunens databehandlere og kommunen som databehandler

Indhenter Norddjurs Kommune en IT-leverandør eller konsulent, som skal behandle personoplysninger på vegne af kommunen, så skal sådanne aftale reguleres af et skriftligt dokument. Dette dokument omtales som en databehandleraftale (efterfølgende omtalt som DBA), og beskriver forholdet mellem den dataansvarlige og databehandleren. For eksempel hvilke ressourcer databehandleren skal stille til rådighed, for at den dataansvarlige kan efterleve sine forpligtigelse til databeskyttelseslovgivningen. Herudover beskriver aftalen blandt andet, hvordan databehandleren må behandle personoplysningerne, og til hvilke underleverandører oplysningerne må videregives.

Det er i starten af 2021 opgjort, at kommunen har overblik over 141 DBA'er[2]. Der er ikke differentieret mellem IT-leverandører og konsulentydelser. Afsøgning om der findes DBA'er, der ikke indgår i det samlede overblik er ikke afsluttet.

Databeskyttelseslovgivningen påbyder den dataansvarlige at påvise ansvarlighed i henhold til persondatabehandlinger. Det betyder i praksis, at

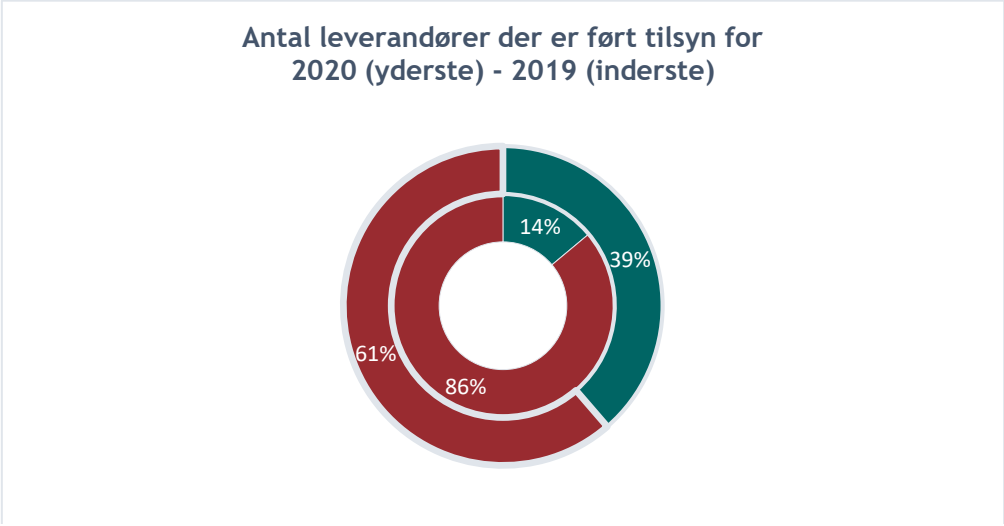


Diagram 1: Antal leverandører der er blevet udført et tilsyn for i henholdsvis 2020 (yderste cirkel) og 2019 (inderste cirkel).

[1] Cookies er små tekstfiler, som bliver lagret i den besøgendes browser. De anvendes fx til at spore den besøgende, så hjemmesiden fungerer korrekt, til statistik, m.m.

[2] De 141 DBA'er fremgår i kommunens IT overblikssystem, KITOS.

den dataansvarlige skal føre tilsyn hos databehandleren på jævnlig basis, og som udgangspunkt én gang om året, medmindre andet er vurderet nødvendigt. Det kan for eksempel være, at den dataansvarlige vurderer, at en lille leverandør, som kun behandler et mindre omfang af almindelige personoplysninger, ikke behøver et årligt tilsyn.

I løbet af det forgangne år, har Norddjurs Kommune indgået et tættere samarbejde med Syddjurs og Favrskov Kommune omkring tilsynsførelse, særligt med henblik på at føre tilsyn hos databehandlere, som alle tre kommuner benytter. Kommunerne kan på den baggrund vinde både tid og ressourcer ift. tilsynsførelsen.

Norddjurs Kommune har i 2020 ført tilsyn for 83 (58 %) ud af de 141 DBA'er. De 141 DBA'er fordeler sig i 2020 på 75 leverandører, hvoraf der er ført tilsyn for 29 (se diagram 1). Dette er en fremgang fra 2019, hvor det blev opgjort, at der var ført tilsyn for 11 leverandører ud af 79. Det skal bemærkes, at medarbejderne som har ført tilsyn for Norddjurs Kommune, under Covid-19 pandemien er stødt på udfordringer med leverandører, som har anvendt pandemien som undskyldning for ikke at tilsende tilsynsmaterialet.

Årsagen til fremgangen mellem 2019 og 2020 er prioritering af yderligere ressourcer til tilsynsområdet, for eksempel i form af virksomhedspraktikanter og en kontraktstyringskonsulent, samt samarbejdet med nabokommunerne.

Der er desuden vedtaget nye retningslinjer og procedurer for Norddjurs Kommunes håndtering af DBA'er. Disse beskriver blandt andet, at der skal foretages en risikovurdering forinden indgåelse af en databehandleraftale. Dette i tråd med Rigsrevisionens rapport om outsourcede persondata (Rigsrevisionen, 2020). Kommunens digitaliseringsafdeling har desuden fået ansvaret for, at der føres tilsyn for samtlige DBA'er som er indgået med IT-leverandører.

I det indledende afsnit blev Schrems II-dommen nævnt. Denne dom omhandlede, at det ikke er tilladt at overføre personoplysninger til USA, på baggrund af 'Privacy-shield[3]' overførselsgrundlaget. Dommen har også betydet, at der er kommet skærpet opmærksomhed på, hvornår dataansvarlige overfører personoplysninger til usikre tredjelande og internationale organisationer. Årsagen til opmærksomheden er særligt, at de usikre tredjelande og internationale organisationer, ikke stiller de samme garantier for et tilstrækkeligt beskyttelsesniveau for de registreredes rettigheder, som

Diagram 2: Antal databehandleraftaler, hvori der overføres personoplysninger til tredjelande eller internationale organisationer. Internationale organisationer er talt med i opgørelsen, da disse ikke nødvendigvis kun er underlagt EU-retten (Datatilsynet, 2019). De internationale organisationer er fx Microsoft, Google og Amazon.

[3] Privacy-shield var en rammeaftale mellem EU og USA, som omhandlede overførsel og sikker behandling af personoplysninger i USA.

databeskyttelseslovgivningen påbyder inden for EU og EØS-landende.

Norddjurs Kommune har opgjort, at det i 56% af DBA'erne fremgår, at der overføres personoplysninger til tredjelande eller internationale organisationer (se diagram 2).

6.2.1.3: Fortegnelser over behandlingsaktiviteter

Artikel 30 i forordningen beskriver, at Norddjurs Kommune skal føre fortegnelser over de persondatabehandlinger 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.

Generelt er fortegnelserne kun til internt brug, medmindre Datatilsynet efterspørger dem.

Norddjurs Kommune påbegyndte revideringen af fortegnelserne i december 2020, og dette arbejde blev afsluttet medio januar 2021. Overordnet har ændringerne været få, for eksempel kan et område have bemærket, at de ikke længere varetager en bestemt type behandling af personoplysninger.

Det skal dog bemærkes, at kommunens fortegnelser *ikke* har taget stilling til, hvorvidt personoplysningerne bliver behandlet i tredjelande. I lyset af den tidligere nævnte Schrems II-dom, er det særligt vigtigt, at kommunen er opmærksom på, hvilke behandlinger der sker i usikre tredjelande, og dette skal derfor indføres i 2021.

Datatilsynet har i 2020 opdateret deres vejledning for fortegnelser over behandlingsaktiviteter. Det skete blandt andet på baggrund af KL's skabeloner til fortegnelser over behandlingsaktiviteters, som Norddjurs ligesom øvrige kommuner har anvendt. Disse KL-skabeloner og behandlingsaktiviteter bliver ajourført ved næste gennemgang af fortegnelserne. Se afsnit 7.3 for den fulde anbefaling.

6.2.1.4: Risikovurderinger og konsekvensanalyser

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

Et fokusområde i 2020 har været risikostyring i hele Norddjurs Kommune. Fokusområdet blev betydeligt forsinket af udbruddet af Covid-19 pandemien. I stedet for at udbrede en risikostyringsmetode til hele organisationen, ændrede fokus sig til at afprøve en risikometode, som er behandlet i Direktionen i marts 2021.

Risikometoden dækker over behandlinger af personoplysninger og IT-aktiver. Formålet er at vurdere hvilke risici der er forbundet med behandlingsaktiviteter og/eller IT-aktiver, for både organisationen såvel som de registrerede. Databeskyttelseslovgivningen påbyder, at der er foretaget en dokumenteret risikovurdering af behandlinger, og at vurderingerne anvendes aktivt, for eksempel ved indgåelse af DBA'er. Risikovurderingen beskriver hvilke risici der er forbundet med en behandling, hvilket tillader Norddjurs Kommune at instruere databehandlere om, hvilke sikkerhedsforanstaltninger de skal implementere.

Risikovurderingen i Norddjurs Kommune bliver omsat til et ledelsesresume. Resumeet indeholder en beskrivelse af risici, anbefalinger til nye sikkerhedsforanstaltninger og afslutningsvis en risikohåndteringsplan, som skal udfyldes af lederen, der er ansvarlig for den pågældende behandling.

I alt er der foretaget risikovurderinger af følgende behandlinger i Norddjurs Kommune under pilottesten:

1. Distancearbejde og hjemmeadgang
2. Norddjurs Kommunes fysiske arkiver,
3. Norddjurs Kommunes kommunaldrev, Outlook og Intranet
4. Skoledu
5. Enversion & Kaunts behandling af fakturaer
6. Office365 (i samarbejde med Syddjurs og Favrskov Kommune)

Ét af formålene med risikostyringen er ligeledes at give Informationssikkerhedsudvalget rapportering om, hvilke risici der befinder sig i organisationen.

Det anbefales fremadrettet, at Norddjurs Kommune fortsat prioriterer risikostyring som et fokusområde. Særligt med henblik på at kvalificere den risikometode, som kommunen har arbejdet med henover 2020. En uddybende anbefaling til fokusområdet kan læses i afsnit 7.1.

6.2.1.5: Sikkerhedshændelser og sikkerhedsbrud

Norddjurs Kommune har pligt til at registrere alle persondatabrud, jævnfør lovgivningen. Hvis disse brud indebærer risici for de registreredes rettigheder, skal de desuden anmeldes til Datatilsynet. Vurderer Norddjurs Kommune desuden, at bruddet indebærer store risici for de registreredes rettigheder, skal kommunen underrette den registrerede om bruddet. En sådan underretning skal beskrive hvad der er sket, hvad kommunen har gjort for at stoppe bruddet, hvilke konsekvenser bruddet kan have for den registrerede såvel som kontaktoplysninger på relevante nøglemedarbejdere. Lækker Norddjurs Kommune ved en fejl helbredsoplysninger om borgere på en hjemmeside, vil dette for eksempel kunne have høje risici for de registreredes rettigheder om privatlivets fred, og den registrerede skal derfor underrettes.

Alle sikkerhedshændelser og persondatabrud skal, jævnfør Norddjurs Kommunes procedure for indberetning af sikkerhedshændelser og persondatabrud registreres, medmindre disse falder under bagatelgrænsen. En sådan bagatel kunne for eksempel være, at en ansat sender ikke-fortrolige personoplysninger til en forkert ansat, eller at en ansat taber sit adgangskort til bygningerne, men umiddelbart herefter får det lukket.

I 2020 har Norddjurs Kommune registreret 55 sikkerhedshændelser, hvoraf 45 er brud på persondatasikkerheden. Til sammenligning blev der i 2019 registreret 20 sikkerhedshændelser, hvoraf 15 var brud på persondatasikkerheden.

Det kan konstateres, at der er sket en positiv stigning i registreringen. Det må forventes, at der sker en yderligere stigning i 2021, imens organisationen fortsat modnes på datasikkerhedsområdet.

Af de 55 sikkerhedshændelser, er der registreret begrænsende foranstaltninger for 48 af hændelserne og nye foranstaltninger for 42 af hændelserne. En begrænsende foranstaltning kan for eksempel være, at en sagsbehandler som har sendt digital post forkert, har bedt den forkerte modtager om at destruere posten. En ny foranstaltning kan være nye tekniske eller organisatoriske tiltag, som skal formindske risikoen for lignende hændelser i fremtiden.

Ud af de 44 sager om brud på persondatasikkerheden, har kommunen i 13 af sagerne valgt at underrette de registrerede om bruddet. Kommunen skal kun underrette de registrerede, hvis bruddet har høje risici for de registreredes rettigheder.

Norddjurs Kommune har anmeldt 22 af de 45 sager til Datatilsynet. Der er anmeldelsespligt til tilsynsmyndigheden, såfremt et brud indebærer risici for den registreredes rettigheder. Med andre ord, har kommunen vurderet i 23 sager, at bruddet ikke har haft konsekvenser for den registreredes rettigheder. Dette kan for eksempel lade sig gøre, når begrænsende foranstaltninger er etableret.

Datatilsynet har ved udgangen af 2020 afsluttet 17 af de 22 sager. I ét tilfælde gav Datatilsynet kritik af Norddjurs Kommunes behandling af personoplysninger.

Af de samlede 55 sikkerhedshændelser, har den primære hændelsestype været fejlagtig offentliggørelse af personoplysninger (se diagram 3). Samlet er der registreret 19 hændelser, som er blevet markeret som fejlagtigt offentliggørelse. Dette er for eksempel på Norddjurs Kommunes hjemmeside i forbindelse med høringssvar, hvor kommunen uden videre offentliggjorde høringssvar, uden at gennemgå svarene for fortrolige oplysninger. Den anden hyppigste hændelsestype har været rigtige oplysninger til en forkert modtager. Denne type hændelse er der registeret 13 af i 2020. Dette kan for eksempel være, hvis en ansat har indtastet et forkert personnummer ved afsendelse af en afgørelse. Desuden er der registreret 5 sager, hvor forkerte oplysninger har været sendt til den rigtige modtager, 4 sager med usikker transmission (usikker post), 2 sager med tab eller tyveri af enheder, 1 sag med generelt datatab og 11 sager markeret som 'andet'. Andet dækker blandt andet brud på kommunens politikker og retningslinjer, ansattes brugere, som ikke er slettet rettidigt eller mistet tilgængelighed til leverandører.

På baggrund af hændelsestyperne anbefales det, at kommunen fortsat arbejder med at sikre, at dens arbejdsgange ift. opbevaring af personoplysninger, er tilstrækkeligt fortrolige. Der kan ikke afgives en konkret anbefaling, da offentliggørelserne af personoplysninger er sket i vidt forskellige scenarier.

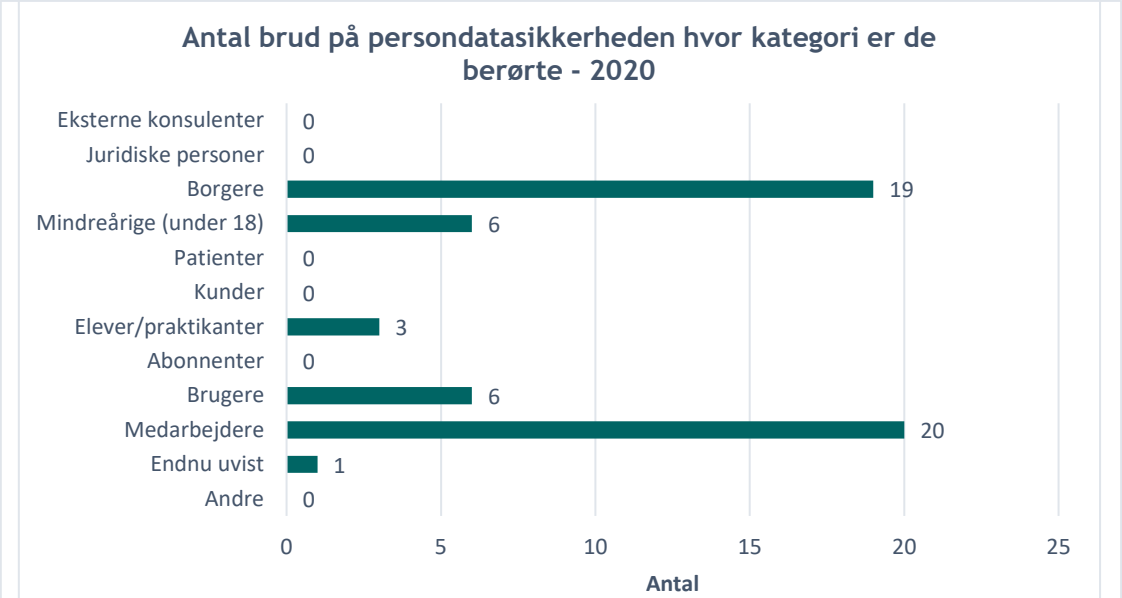


Diagram 3: Antal brud på persondatasikkerheden, hvor en bestemt kategori af registrerede har indgået. 'Endnu uvist' dækker en hændelse, hvor der ikke blev konstateret om der var sket et konkret brud på persondatasikkerheden (intern kilde).

Sikkerhedshændelserne omhandler flere typer af persongrupper (registrerede). De registrerede fordeler sig primært på voksne borgere (19 sager) og medarbejdere (20 sager), men der findes også enkelte sager med mindreårige (se diagram 3). Det er værd at bemærke, at mindreårige (under 18 år) nyder særlig beskyttelse i henhold til databeskyttelseslovgivningen, da børn og unge ikke er i stand til at forstå eller handle på deres persondataretigheder. I 2020 har det primært været Aula, som har offentliggjort for mange almindelige personoplysninger om børn, for eksempel billeder, som er blevet delt med for mange på platformen. Norddjurs Kommune bør fortsat have skærpet opmærksomhed på datasikkerheden i Aula, både under den fortsatte udrulning på Dagtilbudsområdet, såvel som driften på Skoleområdet.

De mest hyppige oplysninger som har indgået i et brud på persondatasikkerheden i 2020, har været registreredes navne, personnumre, fødselsdatoer (som også indgår i personnummeret) og andre typer personoplysninger. Andre typer personoplysninger kan for eksempel være billeder, ferieforhold, forældremyndighed eller lånerstatus på biblioteker.

Covid-19 pandemien har desuden givet anledning til, at en større andel af administrationen og sagsbehandlerne har skulle arbejde hjemmefra. Som tidligere nævnt, kan man opsætte en hypotese om, at der sker flere brud på persondatasikkerheden, når medarbejdere går fra det vante kontormiljø til en distancearbejdsplads. I 2020 er der registreret for 36 hændelser, at 20 af dem er sket på kontoret og 16 af dem på en distancearbejdsplads. De resterende 19 hændelser er ikke opgjort ift. kontor eller distancearbejdsplads. Tallene giver ikke anledning til særlige bemærkninger, udover det kan være værd at analysere nærmere, med et større datagrundlag, om det er bestemte typer hændelser som sker på distancearbejdspladser i modsætning til kontoret.

I Databeskyttelsesrådgiverens årsrapport for 2019 var ét fokusområde at øge registreringen af sikkerhedshændelser og -brud. Det kan konkluderes, at kommunen har mere end fordoblet denne registrering i 2020. Desuden er der udarbejdet ledelsesstatistikker (som blandt andet er set i de ovenstående diagrammer), der tillader kommunens ledelse at prioritere ressourcer på de mest graverende områder. Desto større datagrundlag kommunen skaber, desto bedre vil ressourcerne kunne fordeles og awareness arbejdet struktureres. Det anbefales derfor fortsat, at der er fokus på registreringen af både hændelser og brud på persondatasikkerheden, og at ledelsesafrapporteringen fortsat kvalificeres.

6.2.1.6: Awarenesstiltag

Der er i løbet af 2020 blevet udført fem centrale awarenesstiltag, for at øge opmærksomheden omkring datasikkerhed.

1) Spørgeskemaundersøgelse om databeskyttelse og informationssikkerhed (februar, 2020)
2) Kampagne med skrivebordsbaggrunde og budskaber (forår og efterår, 2020)
3) Podcasts om databeskyttelse (sommer, 2020)
4) Informationsmateriale om databeskyttelse på kommunens intranet (august, 2020)
5) Genudsendelse af kommunens e-læringskursus om databeskyttelse (november og december, 2020)

Udover de større tiltag, har der løbende været fokus på, hvordan datasikkerheden bedst håndteres på distancen.

Spørgeskemaundersøgelsen omhandlede personalets viden om kommunens politikker og procedurer, samt generel viden om databeskyttelse og informationssikkerhed. Resultaterne viste, at personalet havde ønsker til mere viden om databeskyttelse og informationssikkerhed.

Skrivebordskampagnerne, der rammer alle i organisationen, som anvender Citrix blev gennemført i to faser.

Den første fase af kampagnen indeholdt fem budskaber som kørte hen over personalets skriveborde i en periode af 10 uger. Budskaberne omhandlede i foråret:

- Vi lader ikke data flyde
- Vi låser altid vores PC
- Vi sender data sikkert
- Vi er kreative med passwords
- Vi henter samtykke når nødvendigt

Anden fase af kampagnen blev igangsat i uge 38, og ligesom første fase, indeholdt den fem nye budskaber og løb i 10 uger. De fem budskaber i efteråret:

- Vi rydder op i vores data
- Vi informerer borgerne om deres rettigheder
- Vi opbevarer personoplysninger sikkert – og følsomme ekstra sikkert
- Vi falder ikke for phishing
- Vi tager kun billeder – når vi har lov

I løbet af sommerperioden blev der udgivet tre podcasts om databeskyttelse, som også ligger tilgængelig på intranettet. Metoden blev valgt, for at give ansatte et nemt alternativ til at sætte sig ind i de mere grundlæggende temaer om databeskyttelse. Konkret omhandlede de tre podcasts:

- Hvad er personoplysninger
- Hvornår må du behandle personoplysninger
- Samtykke

Det er intentionen at udvide podcast-porteføljen i 2021 til flere grundlæggende emner.

Intranettet blev taget i anvendelse i 2020. Det har derfor været en selvstændig awareness-indsats at stille materiale om informationssikkerhed og databeskyttelse til rådighed på intranettet. Ligesom Norddjurs Kommunes andre kommunikationsplatforme, vil indholdet om databeskyttelse på intranettet løbende blive ajourført med nye vejledninger, procedurer og awareness-materiale.

Årets afsluttende awareness-tiltag var at genudsende kommunens e-læringskursus om databeskyttelse, hvor kursets indhold var tilpasset brugernes behov på forskellige niveauer. Enkelte personalegrupper har valgt at modtage information på anden måde, for eksempel personalemøder. Det er oplevelsen, at diverse kampagner, der har suppleret hinanden, generelt har øget awarenessniveauet i kommunen.

I afslutningen af 2020 blev det aftalt i Informationssikkerhedsudvalget fremover at inddrage fagområderne mere i forbindelse med udarbejdelsen af awareness- og opkvalificerende materiale for at tilgodese særlige behov forskellige steder i organisationen.

Databeskyttelsesrådgiveren anser fokusområdet fra årsrapport 2019 vedr. awarenesstiltag opnået på kort sigt, men fremhæver samtidig, at arbejdet med awareness og kampagner bliver tilbagevendende begivenheder.

6.2.1.7: Kontrol og opfølgning på arbejdet

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

År 2020 har været et særligt år for det egentlige tilsynsarbejde. Det har været første år med konkrete tilsyn og det har været et år præget af Covid-19. Tilsynene der blev ført i februar-juni perioden var baseret på interne notater, der for eksempel bad chefen dokumentere, at en pågældende afdeling havde kendskab til kommunens in-

formationssikkerhedspolitikker, eller at afdelingen havde tilstrækkelig brugerstyring i sine IT-systemer.

Overordnet fulgte tilsynene en model, hvor formålet både var at føre internt tilsyn, men specielt også at komme med anbefalinger og læring til fagområdet. Udgangspunktet var at kunne dokumentere efterlevelsen af databeskyttelsesforordningen (se model 1). Modellen forholdt sig til lovgivningens artikler, der blev operationaliseret til spørgsmål, som kunne besvares med relevant dokumentation. Herunder, at der var udformet konkrete retningslinjer og at de blev overholdt.

For eksempel påbyder lovgivningen, at kommunen indgår databehandleraftaler med leverandører, som behandler personoplysninger på vegne af kommunen. Har Norddjurs i den forbindelse, udformet retningslinjer for indgåelse af aftalerne og tilsyn med leverandørerne, og kan kommunen dokumentere, at retningslinjerne overholdes.

I alt blev der i februar-juni perioden udsendt 31 kontrolaktiviteter til organisationen. På baggrund af drøftelser om metode blev det aftalt, at kontrolaktiviteter skulle suppleres med mere vejledning før en kontrol, blev sat i værk.

Konklusionen af de førte kontroller var primært, at afdelingerne ikke havde decentrale retningslinjer for håndtering af databeskyttelse, og at de ønskede mere central styring på området. Det resulterede blandt andet i styringsdokumentet: Norddjurs Kommunes tværgående retningslinjer for informationssikkerhed.

Det blev konstateret, at dokumentation af brugerstyring i fagsystemer kunne forbedres. Derfor anbefales det, at IT-systemer og brugerrettigheder er et fokusområde i 2021 (se afsnit 7.2 for uddybelse).

Ved årsskiftet 2020/2021 blev det første fysiske tilsyn udført i Borgerservice. Tilsynet var både konkret, men også et pilotforsøg på fysiske tilsyn fremover. Der blev i den anledning ikke registreret særlige bemærkninger, og ledelsen bemærkede til oplevelsen, at det var en god øvelse, der er med til at fastholde fokus på informationssikkerheden og opbevaring af persondata.

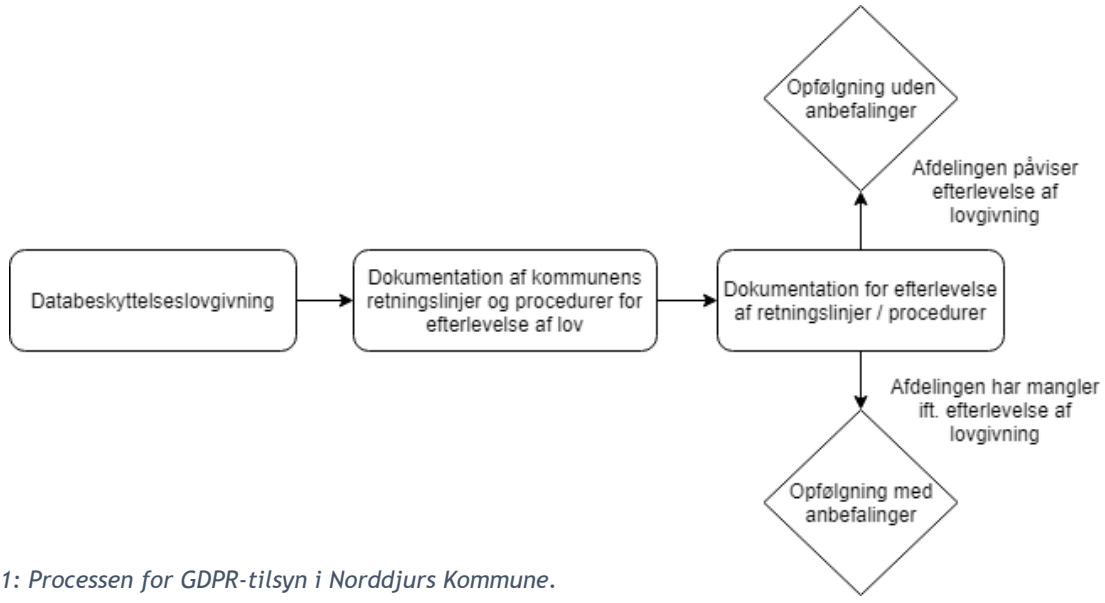
Den nye tilgang til kontrolarbejdet i Norddjurs Kommune baserer sig fortsat på model 1, men fremover med inddragelse af området inden tilsynet igangsættes.

6.2.2: Nye artikler og lovgivning i fokus for årsrapport 2020

6.2.2.1: Principper for behandling af personoplysninger

Databeskyttelsesforordningens artikel 5, beskriver de grundlæggende principper for behandling af personoplysninger. Principperne er, at personoplysninger skal:

1. behandles lovligt, rimeligt og gennemsigtigt
2. behandles til udtrykkeligt angivne formål (formålsbegrænsning)
3. være tilstrækkeligt relevante og begrænset til formålet (dataminimering)
4. være rigtige



Model 1: Processen for GDPR-tilsyn i Norddjurs Kommune.

5. opbevares med en defineret slette- eller arkiveringsfrist (opbevaringsbegrænsning)
6. behandles sikkert, så de ikke ændres eller lækkes (integritet og fortrolighed)

Norddjurs Kommune skal kunne dokumentere, at organisationen overholder de 6 principper, jævnfør artikel 5, stk. 2.

Derfor har Norddjurs Kommune udarbejdet en vejledning og tjekliste, som kan anvendes ved opstart af nye projekter der behandler personoplysninger. Dokumentet operationaliserer de ovenstående principper, så ledelse, projektledere eller andre relevante grupper kan forholde sig til, hvorvidt de overholder principperne.

6.2.2.2: Lovlighed af behandling af personoplysninger

Artikel 6, 9 og 10 i forordningen beskriver, hvornår dataansvarlige må behandle personoplysninger lovligt[4]. Artikel 6 omhandler behandling af almindelige personoplysninger. Artikel 9 omhandler behandling af følsomme personoplysninger. Og artikel 10 omhandler behandling af personoplysninger vedr. strafbare forhold.

Overordnet er der i 2020 ikke konstateret reelle problemer med lovligheden af Norddjurs Kommunes behandlinger. Størstedelen af kommunens behandlinger er for eksempel lovlige jævnfør serviceloven, sundhedsloven, bekendtgørelse om en aktiv beskæftigelsesindsats, osv. Med andre ord, har forvaltningen hjemmel til at udføre sit virke ifølge faglovgivning på de enkelte områder.

Det er dog konstateret, at der kan være situationer, hvor der opleves usikkerhed med, hvornår der skal indhentes samtykke fra de registrerede. Det kan for eksempel være institutioner der vil tage billeder af elever, brugere, m.m. Problematikken om samtykke er imidlertid ikke afgrænset til Norddjurs Kommune, og det kan i mange tilfælde være svært at vurdere, hvorvidt en behandling af for eksempel billeder kræver samtykke. Opmærksomhed på problemstillingen er dog et væsentligt skridt til at opfylde kravene til samtykke. Det er samtidig et område, hvor informationssikkerhedskoordinatoren kan kontaktes for vejledning om reglerne.

[4] Der findes også retsgrundlag i den supplerende danske databeskyttelseslov. Disse retsgrundlag er ikke i fokus i denne afrapportering.

6.2.2.3: Persondatarettighederne

Kapitel 3 i databeskyttelsesforordningen omhandler den registreredes rettigheder. Heri beskrives blandt andet, at den registrerede har ret til at blive oplyst om en behandling, når den registreredes personoplysninger indsamles (se evt. afsnit 6.2.1.1). Herudover fremgår rettighederne om indsigt i behandlingen af personoplysninger, berigtigelse og sletning af personoplysninger, begrænsning af behandling, retten til dataportabilitet og retten til indsigelse. Rettighederne er en blanding af nogle den dataansvarlige aktivt skal afgive til den registrerede (oplysningspligten), og rettigheder som den registrerede selv aktivt skal anvende.

I 2020 har Norddjurs Kommune formaliseret procedurer for samtlige af ovenstående rettigheder. Procedurerne beskriver, hvordan kommunen skal håndtere efterlevelsen af rettighederne samt skabeloner der kan hjælpe med at løfte opgaven. Procedurerne er:

- Oplysningspligten
- Retten til indsigt
- Retten til berigtigelse
- Retten til sletning
- Retten til begrænsning af databehandling
- Retten til dataportabilitet
- Retten til indsigelse

Der er ikke registreret konkrete henvendelser fra hverken borgere eller ansatte i 2020, som har ønsket at gøre brug af deres persondatarettigheder.

6.2.2.4: TV-overvågning i Norddjurs Kommune

Folketinget vedtog den 28. maj 2020 en ændring af lov om TV-overvågning. Lovændringen betød, at det blev nemmere for offentlige myndigheder at anvende videoovervågning. Desuden skulle kameraer, som overvåger gade, vej, plads eller lignende områder, som benyttes til almindelig færdsel, registreres i politiets register over TV-overvågning (POLCAM).

På den baggrund igangsatte Norddjurs Kommune en intern undersøgelse af, hvor mange videokameraer kommunen besidder, hvad formål og rets-

grundlag er for disse, kameraets placering, hvorvidt det er registreret i POLCAM (Politiets register), hvordan det optagede videomateriale behandles, hvornår materialet slettes, adgangsrettigheder til det filmede og oplysning om, hvordan de registrerede bliver orienteret om overvågningen.

Konklusionen af undersøgelsen var, at ved udgangen af 2020 havde Norddjurs Kommune opsat 99 videokameraer i afdelinger og institutioner. Arbejdet med at få alle relevante kameraer registreret fortsætter ind i 2021.

Alle videokamera er opsat med henblik på kriminalitetsbekæmpelse, eller som en foranstaltning imod tyveri og hærværk.

TV-overvågning ved samtlige videokameraer bliver skiltet på døre eller vægge nær videokameraet. Skiltningen beskriver, at området er videoovervåget, men der udestår fortsat en opgave med at oplyse om formålet med skiltning, hvilket for eksempel kan ske med QR-koder. Dette område vil der fortsat være fokus på i forbindelse med registrering og ajourføring af registeret over TV-overvågning, herunder opbevaring af videooptagelser.

7. Databeskyttelsesrådgiverens anbefalinger til fokusområder i 2021

For at Norddjurs Kommune fortsat kan have succes med at skabe en god databehandlingskultur i 2021, har Databeskyttelsesrådgiveren identificeret de følgende fire fokusområder:

1. Risikostyring i hele Norddjurs Kommune
2. IT-systemer og brugerrettigheder
3. Fortegnelser over behandlingsaktiviteter
4. Valg af databehandlere og tilsyn med disse

Nedenfor vil de fire fokusområder blive gennemgået i dybden.

7.1: Risikostyring i hele Norddjurs Kommune

Målgruppen for denne anbefaling er særligt Informationssikkerhedsudvalg, systemejere og projektledere.

Databeskyttelseslovgivningen påbyder, at Norddjurs Kommune kan påvise, at personoplysninger behandles sikkert. Dette blandt andet ved, at kommunen har foretaget en struktureret og metodisk overvejelse om, hvilke risici en registrerets rettigheder og frihedsrettigheder kan udsættes for, når en given behandling af deres oplysninger finder sted.

I første kvartal af 2021 står Norddjurs Kommune til at vedtage en risikometode for organisationen. Den risikometode bliver udgangspunkt i kommunens fortsatte arbejde med risikostyring, og giver kommunen en struktureret og metodisk tilgang til vurdering af risici.

Databeskyttelsesrådgiveren anbefaler på den baggrund, at Norddjurs Kommune prioriterer sine behandlingsaktiviteter ud fra følgende parametre, og dernæst udfører en risikovurdering på behandlingsaktiviteter. De mest sårbare områder skal prioriteres og risikovurderes først.

1. Behandling af personoplysninger med fortrolig eller følsom karakter
2. Behandling af en stor mængde personoplysninger
3. Behandling af personoplysninger om børn
4. Behandling af personoplysninger om sårbare
5. Automatisk behandling som profiling, der giver grundlag for beslutninger med lovmæssig effekt eller lignende effekt
6. Større skala af systematisk overvågning af offentlige rum
7. Anvendelse af ny teknologi
8. Personoplysningerne bliver overført til usikre tredjelande eller internationale organisationer

Målet for Norddjurs Kommune bør være, at de relevante behandlingsaktiviteter, skal være risikovurderet inden for et rimeligt tidsrum, som løbende vurderes og aftales som en del af processen.

7.2: IT-systemer og brugerrettigheder

Målgruppen for denne anbefaling er særligt kommunens Informationssikkerhedsudvalg og systemejerne.

En grundlæggende sikkerhedsforanstaltning for beskyttelse af personoplysninger, hvad end de er

i fysiske eller digitale arkiver, er styring af adgangsrettigheder til oplysningerne. Et af principperne i en god databehandlingskultur er, at det *kun* er de medarbejdere, der skal anvende oplysningerne, som skal have adgang til dem. Formålet skal være arbejdsrelateret.

Norddjurs Kommune skal have retningslinjer for brugerrettigheder i de enkelte IT-systemer, som behandler personoplysninger. Hvilke personoplysninger findes i systemet, hvem må få adgang til oplysningerne og hvorfor samt en opfølgning på de udstedte adgange.

Databeskyttelsesrådgiveren anbefaler på den baggrund, at Norddjurs Kommune danner sig et overblik over IT-systemer på fagområderne og sikrer:

1. Retningslinjer for tildeling, opdatering og nedlæggelse af medarbejderadgange i IT-systemet
2. Autorisationskontrol i IT-systemet, herunder hyppighed af kontrol
3. Hvorvidt brugerhandlinger logges i IT-systemet, og om disse logfiler bør kontrolleres for utilsigtede hændelser

7.3: Fortegnelser over behandlingsaktiviteter

Norddjurs Kommune skal føre fortegnelse over sine behandlingsaktiviteter af personoplysninger. Indtil videre har kommunen anvendt KL's skabeloner. Datatilsynet har i 2020 opdateret sin vejledning for fortegnelser, hvilket giver anledning til at genbesøge de foreliggende fortegnelser baseret på KL's oprindelige skabeloner.

Det anbefales derfor, at Norddjurs Kommune prioriterer at udforme nye fortegnelser over behandlingsaktiviteter, med udgangspunkt i Datatilsynets vejledning.

7.4: Valg af databehandlere og tilsyn med disse

Målgruppen for denne anbefaling er særligt informationssikkerhedsudvalget og systemejere.

Schrems II-dommen satte overførsler til usikre tredjelande og internationale organisationer på dagsordenen i 2020. Dette for at sikre, at de registreredes rettigheder ikke blev kompromitteret, når en dataansvarlig eller databehandler overfører personoplysninger til usikre tredjelande.

Norddjurs Kommune har ved årsskiftet 2020/2021 skabt overblik over databehandleraftaler, der indeholder overførsler til usikre tredjelande.

Databeskyttelsesrådgiveren anbefaler på den baggrund, at Norddjurs Kommune gennemgår databehandleraftaler og forholder sig til de anbefalinger, som KL har udsendt til kommunerne i februar måned 2021.

.

8. Konkluderende bemærkninger

Formålet med statusrapporten er at give svar på:

Hvordan er Norddjurs Kommunes tilstand med databeskyttelsesarbejdet i 2020?

Hvordan har det udviklet sig siden 2019?

Hvilke fokusområder anbefaler databeskyttelsesrådgiveren, at kommunen fremadrettet arbejder med?

Databeskyttelsesarbejdet har udviklet sig betydeligt i løbet af 2020, uden større påvirkning af Covid-19 og nedlukning af samfundet. Norddjurs Kommune har struktureret organisering og ansvar af informationssikkerhedsarbejdet, arbejdet med risikometode, der passer til kommunen, udført større awareness-tiltag og har over fordoblet sine registreringer af sikkerhedshændelser og persondatabrud fra 2019. Dertil kommer en lang række indsatser, der har været med til at udvikle databehandlingskulturen og dokumentere dette.

Databeskyttelsesrådgiveren har i løbet af året observeret medarbejdernes øgede fokus på informationssikkerhed og databeskyttelse.

Mange nye administrative procedurer, værktøjer og skabeloner er blevet udarbejdet i 2020, som skal hjælpe forvaltningen med at efterleve databeskyttelseslovgivningen.

Der er imidlertid fortsat behov for at fastholde fokus på de gode forbedrede rutiner, der udgør rygraden i den gode og solide databehandlingskultur. Ligesom der på enkelte områder fortsat skal arbejdes for at få et passende og tilstrækkeligt niveau for informationssikkerhed og databeskyttelse.

Derfor anbefaler databeskyttelsesrådgiver i 2021 følgende fokusområder:

1. Risikostyring i hele organisationen
2. IT-systemer og brugerrettigheder
3. Fortegnelser over behandlingsaktiviteter
4. Valg af databehandler og tilsyn med disse

De fire fokusområder er udvalgt på baggrund af den samlede status på området samt nye vejledninger fra Datatilsynet.

Det blev i årsrapporten for 2019 bemærket, at den gode databehandlingskultur forventeligt vil tage flere år, før den endeligt er forankret og i drift. Norddjurs Kommune er i 2020 kommet rigtig langt med at opnå denne målsætning.