norddjurs kommune

DATABESKYTTELSESRÅDGIVERENS

ÅRSRAPPORT 2025

Indhold

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 2025 følger derfor op på fokusområder i den tilsvarende rapport for 2024 med anbefalinger til kommende år.

3. Metode

Årsrapporten beskriver generelt og overordnet kommunens status for arbejdet med informationssikkerhed og databeskyttelse. Indholdet bygger på databeskyttelsesrådgiverens observationer og kontroller samt organisationens 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 i Complianceteamet af en databeskyttelseskoordinator og suppleres af kommunens informationssikkerhedskoordinator og -konsulenter.

5. Det forgangne år – 2025

Afsnittet giver indsigt i kommunens arbejde med informationssikkerhed og beskyttelse af persondata 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 Ajourføring af fortegnelser

Det seneste år har der været travlhed inden for complianceområdet, både i forbindelse med databeskyttelse, Den Gode IT-anskaffelse samt NIS2[1], og arbejdet med fortegnelser har derfor været nedprioriteret. Det er forventningen, at opgaven med ajourføring af fortegnelser inden for nærmeste fremtid kan blive prioriteret igen.

5.1.2 Videreudvikling af Den Gode IT-anskaffelse

Den Gode IT-anskaffelse er blevet den fælles indgang for nye it-systemer i Norddjurs Kommune, og flere løsninger kommer nu korrekt gennem processen – blandt andet understøttet af Exit-Citrix-projektet, hvor medarbejdere ikke længere selv kan installere programmer.

Der er dog fortsat eksempler på, at it-systemer anskaffes eller web-baserede løsninger anvendes uden forudgående involvering af Complianceteamet, hvilket udfordrer overblik, integrationer og databeskyttelse. Den Gode IT-anskaffelse understøtter de krav, der følger af NIS2, herunder styrket styring af systemportefølje og leverandører. Der findes vejledninger på intranettet, og Complianceteamet vil fremover tilbyde at komme ud til både ledere og medarbejdere for at holde oplæg om formål, ansvar og praktisk brug af Den Gode IT-anskaffelse.

5.1.3 Datatilsynets fokusområder i det forgangne år: Beskyttelse af børn, registreredes ret til sletning samt kunstig intelligens

Datatilsynets fokusområder har i 2025 været omdrejningspunkt i både skriftligt og fysisk tilsyn i fagområderne. Dermed har Complianceteamet fået indblik i, hvordan de forskellige fagområder forholder sig til de relevante problematikker, samt hvordan der kan arbejdes videre med det i kommende år.

Arbejdet med rettighedsstyring og brugeradministration er fortsat i gang, så det er i særdeleshed vigtigt at have fokus på dette, når der behandles fortrolige og følsomme personoplysninger – herunder også om børn og unge under 18 år.

Derudover skal der fremadrettet være øget fokus på borgeres anmodninger om indsigt og sletning af data. Der gælder særlige regler for disse anmodninger, som adskiller sig fra for eksempel aktindsigt. Dette skal både medarbejdere og ledelse være informerede om, så anmodningerne behandles korrekt.

Til sidst har der i det forgangne år været stort fokus på kunstig intelligens på tværs af kommunen. Flere og flere it-systemer er begyndt at introducere funktioner med kunstig intelligens, ligesom Copilot er ble-

[1] NIS2 er et EU-direktiv og dansk lovgivning, der har til formål at styrke og ensarte cybersikkerheden, så blandt andet kommuner bedre kan modstå cyberangreb og beskytte kritiske it-systemer.

vet en fast "samarbejdspartner" for mange ansatte. Det er derfor vigtigt, at alle medarbejdere er bevidste om regler og risici i forbindelse med arbejdet med kunstig intelligens. Det vil Complianceteamet derfor fortsat have fokus på.

5.2 Status på andre fokusområder i det forgangne år

Herunder samles der op på andre områder, der har fyldt meget i arbejdet med databeskyttelse i 2025.

5.2.1 Konsekvensanalyser

I 2025 har udbredelsen af kunstig intelligens medført et øget fokus på konsekvensanalyser. Konsekvensanalyser er en central del af kommunens arbejde med behandling af store mængder personoplysninger og følsomme data, implementering af nye it-systemer og anvendelsen af AI.

Konsekvensanalyser er afgørende for at sikre overholdelse af GDPR og AI-forordningen, samtidig med at de hjælper med at identificere og reducere risici for borgernes rettigheder. Derudover bidrager de til, at kommunen kan dokumentere ansvarlig og lovmedholdelig datahåndtering. Konsekvensanalyser er ofte tidskrævende og kan derfor være en længere proces. De indgår som et fast element i kommunens proces for Den Gode IT-anskaffelse, selvom der ikke altid er ressourcer til at udarbejde dem før ibrugtagen af alle nye it-systemer, så udarbejdes de efterfølgende.

5.2.2 Logning og stikprøvekontroller

Logning og stikprøvekontroller har været et gennemgående fokusområde i 2025. Loggen anvendes til at dokumentere ændringer i journaler og sager og giver samtidig mulighed for at kontrollere medarbejderes adfærd. Derfor anbefaler Complianceteamet, at fagområderne løbende udfører stikprøvekontroller i it-systemer, der behandler fortrolige og følsomme personoplysninger. Formålet er ikke at finde fejl, men at forebygge uretmæssig adgang til data.

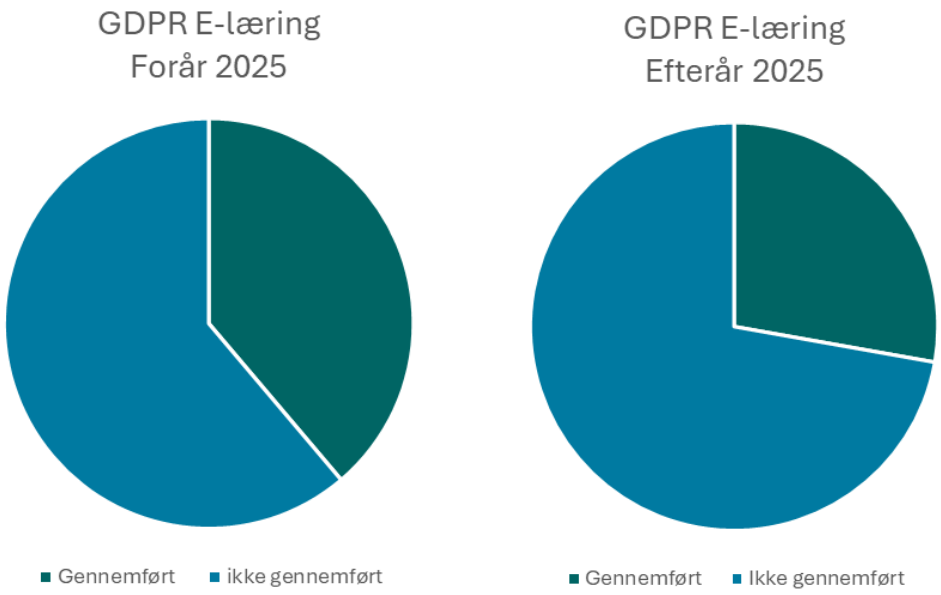
For at sikre gennemsigtighed i databehandlingen – herunder hvilke medarbejdere der tilgår oplysninger – er det afgørende, at vi har adgang til logfunktionalitet i alle vores it-systemer. I praksis er der dog udfordringer, da vi ikke har adgang til logs på alle it-systemer, og fordi adgangen i mange tilfælde er forbundet med omkostninger. Dette kan vanskeliggøre fagområdernes mulighed for at overholde GDPR. Samtidig bliver logadgang stadig vigtigere, når borgere søger indsigt i logoplysninger – en problemstilling, der er stigende i mange kommuner.

5.2.3 Awareness og E-læring

I 2025 blev det besluttet, at der fremover skal udsendes obligatorisk e-læring til alle medarbejdere to gange om året. Beslutningen bygger på øget behov for fokus på databeskyttelse samt yderligere krav om

awareness omkring IT-sikkerhed i forbindelse med implementeringen af NIS2 i kommunerne. Som det ses nedenfor, føres der statistik på gennemførsel på tværs af kommunen. I foråret 2025 var der en gennemførselsprocent på 38,8 %, mens der i efteråret var 27,8 % af kommunens medarbejdere, der gennemførte e-læringen om GDPR. Målet er, at 80 % af alle medarbejdere skal gennemføre e-læringen, hver gang den udsendes.

Derfor vil e-læring og awareness generelt også være et fokusområde i 2026 som beskrevet yderligere i punkt: 6.2.1 på side 8.



5.3 Sikkerhedshændelser og -brud

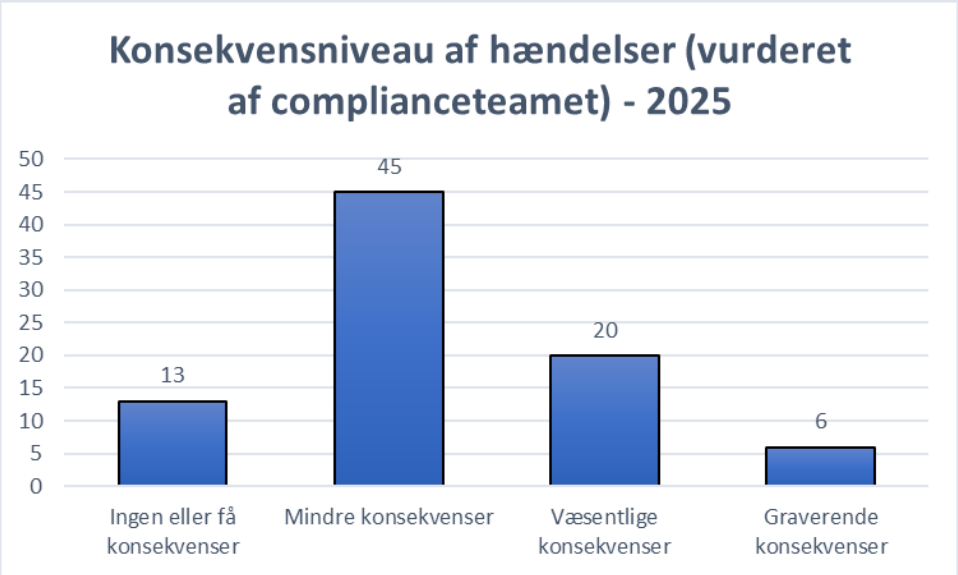
Norddjurs Kommune er forpligtet til at registrere alle sikkerhedsbrud og -hændelser. Hvis et brud indebærer risiko for de registreredes rettigheder, skal det endvidere anmeldes til Datatilsynet, og ved alvorlige risici skal de berørte borgere desuden underrettes.

I 2025 registrerede Norddjurs Kommune i alt **84 sikkerhedshændelser og -brud**. Heraf blev **36** anmeldt til Datatilsynet.

Den hyppigste årsag til brud var **utilsigtet videregivelse**, typisk i form af e-mails med personoplysninger sendt til forkerte modtagere.

Antallet af registrerede hændelser er på niveau med tidligere år og udtryk for medarbejdernes opmærksomhed omkring sikkerhedsbrud og registreringspraksis.

I 2025 blev der registreret **seks brud**, som potentielt kunne medføre alvorlige konsekvenser for de berørte. Ved sådanne sager orienterer Complianceteamet løbende chefen for Borgerservice, IT og Digitalisering samt direktionen.



6. Anbefalinger til fokusområder i 2026

I det følgende beskrives både anbefalinger fra Norddjurs Kommunes databeskyttelsesrådgiver samt relevante fokusområder fra Datatilsynet til 2026.

6.1 Datatilsynets anbefalinger til fokusområder i 2026

Anbefalingerne i dette afsnit er baseret på Datatilsynets særlige fokusområder for tilsynsaktiviteter i 2026.

Overvågning gennem nye teknologier

Kunstig intelligens (AI) til overvågning og kontrol af borgere i pleje

Brugen af kunstig intelligens vokser hurtigt, også i Norddjurs Kommune. Kunstig intelligens kan give bedre beslutningsstøtte og nye muligheder i for eksempel sundheds- og ældreplejen, men teknologien kan også skabe bekymringer og betydelige databeskyttelsesrisici – især for borgere, som ikke kan fravælge disse nye teknologier.

Datatilsynet vil i 2026 derfor have særligt fokus på anvendelse af beslutningsstøttende kunstig intelligens i sundhedssektoren samt kunstig intelligens, der bruges til overvågning og kontrol af borgere i pleje.

Vi skal derfor være ekstra opmærksomme på, at løsningerne, der benyttes i Norddjurs Kommune, er lovlige, nødvendige og proportionale.

Måle- og overvågningsenheder til patientbehandling i hjemmet

Der bruges i stigende grad internetforbundne enheder som sensorer, kameraer og måleinstrumenter i behandlings- og plejeindsatser i borgernes hjem. Datatilsynet oplever, at brud på persondatasikkerheden ofte skyldes uautoriseret adgang til netop sådant udstyr.

IoT-enheder[2] indsamler ofte store mængder data – nogle gange persondata – hvilket stiller krav til datasikkerhed, kryptering og korrekt håndtering efter GDPR. I 2026 vil Datatilsynet derfor gennemføre tilsyn med brugen af IoT-enheder i hjemmebehandling, da området kan udfordre borgernes ret til privatliv – og borgerne har ofte begrænsede muligheder for at sige nej til udstyret.

Overvågning af ansatte

Nye teknologier gør det muligt for kommuner at overvåge medarbejdere på mange måder. Det betyder, at der ofte behandles store mængder personoplysninger, og medarbejdere kan opleve overvågning som både indgribende og svær at sige nej til.

Datatilsynet undersøgte i 2024, hvordan arbejdsgivere overvåger ansatte. På baggrund af denne kortlægning vil Datatilsynet i 2026 gennemføre målrettede tilsyn for at sikre, at kommuner og andre arbejdsgivere overholder reglerne, når de bruger overvågning og kontrollerer medarbejdere.

Overvågning af ansatte er blandt andet relevant for Norddjurs Kommune i forbindelse med tv-overvågning samt flådestyring i kommunens køretøjer med GPS-udstyr.

Danske hjemmesiders sporing af borgere

Mange hjemmesider indsamler store mængder oplysninger uden, at borgerne reelt kan sige nej til sporingsteknologier. Det er derfor et område, som Datatilsynet vil fokusere på og føre tilsyn med.

Norddjurs Kommune skal være opmærksomme på dette, når kommunen driver hjemmesider eller løsninger, der bruger cookies eller andre sporingsmekanismer. Datatilsynets arbejde sker i tæt koordinering med Digitaliseringsstyrelsen, som også fører tilsyn på området.

[2] Internet of Things:
IoT handler om, at fysiske enheder – for eksempel sensorer – bliver forbundet til internettet, så de kan indsamle data, kommunikere, og i mange tilfælde handle automatisk.

Persondatasikkerhed, de registreredes rettigheder og andre særlige tilsynsforpligtelser

Sikker anvendelse af auto-complete[3]

Datatilsynet modtager hvert år mange anmeldelser om brud på persondatasikkerheden, hvor en e-mail er sendt til en forkert modtager. Disse fejlforsendelser kan få alvorlige konsekvenser, når borgeres fortrolige oplysninger havner de forkerte steder. Derfor skærpede Datatilsynet i 2023 reglerne for myndigheders brug af "auto-complete" i e-mailprogrammer.

Det betyder blandt andet, at vi som kommune kun må bruge auto-complete, hvis der er foretaget en risikovurdering og indført tekniske løsninger, der reducerer risikoen for at sende e-mails til forkerte modtagere.

Selvom Datatilsynet siden har udsendt vejledninger, blandt andet om typiske brud på persondatasikkerheden, modtager tilsynet stadig mange anmeldelser om fejlforsendelser. Derfor vil Datatilsynet i 2026 gennemføre målrettede tilsyn – også i kommuner – hvor der behandles store mængder følsomme eller fortrolige personoplysninger, og hvor risikoen ved e-mailfejl er særlig høj.

6.2 Databeskyttelsesrådgiverens anbefalinger til fokusområder i 2026

Anbefalingerne i dette afsnit er baseret på databeskyttelsesrådgiverens egne observationer og vurderinger af konkrete behov i Norddjurs Kommune. Nedenstående taler desuden direkte ind tidligere nævnte fokus- og indsatsområder, som både kommer fra Datatilsynet og Complianceteamet.

6.2.1 E-læring

Som beskrevet i punkt 5.2.3 vil e-læring være et fokusområde for Complianceteamet i det kommende år. Gennemførselsprocentdelen skal op på mindst 80 %, og dette kræver en øget indsats fra både Complianceteamet samt ledelsen. Det er vigtigt, at medarbejdere deltager aktivt i e-læringsmodulerne, både når det omhandler GDPR og IT-sikkerhed generelt.

Derfor vil Complianceteamet i det kommende år have meget mere fokus på formidling af awareness og synlighed i organisationen, som forhåbentlig kan hjælpe med at øge deltagelsen i e-læringen.

6.2.2 Awareness og øget synlighed i organisationen

I forlængelse af ovenstående punkt vil Complianceteamet i 2026 mere ud i organisationen. Vi vil tilbyde at besøge de forskellige afdelinger og holde oplæg om databeskyttelse, informationssikkerhed og Den Gode

[3] Norddjurs Kommune anvender auto-complete til automatisk at foreslå modtagere, når en bruger begynder at indtaste en e-mailadresse eller et navn i feltet Til, Cc eller Bcc i Outlook.

IT-anskaffelse. Målet er at være mere synlige, møde fagområderne dér hvor de er, og tage fat i de udfordringer, der er relevante for netop deres arbejde. Vi forventer, at den direkte dialog kan gøre det nemmere at få styr på reglerne i praksis og skabe en bedre fælles forståelse på tværs af organisationen.

6.2.3 NIS2: Styrket cybersikkerhed, hændelsesrapportering og ledelsesansvar

NIS2 er et EU-direktiv om IT-sikkerhed, som trådte i kraft 1. juli 2025 via den danske NIS2-lov. Kommunerne er omfattet af denne lovgivning og dermed underlagt skærpede krav til beskyttelse af data og digitale it-systemer mod cyberangreb. For at kunne opfylde kravene for NIS2, kræver det en kortlægning af it-systemer, opdatering af politikker og uddannelse af medarbejdere og ledelse.

I løbet af 2026 vil NIS2 derfor være et fokusområde for arbejdet med at sikre data, digitale it-systemer og infrastruktur. Vi vil forsætte arbejdet med at beskytte alle it-systemer, opdage, håndtere og rapportere sikkerhedshændelser indenfor 24 timer og sætte krav til leverandørernes sikkerhed. Ligeledes vil der være fokus på det ledelsesmæssige ansvar, som der stilles krav til i NIS2-loven.

Alle ansatte i Norddjurs Kommune har en rolle i beskyttelse af den kommunale organisation ved at være opmærksomme på IT-sikkerhed gennem forsvarlig håndtering af data, opmærksomhed på mistænkelige mails og anvendelse af stærke adgangskoder.

7. Konkluderende bemærkninger

Formålet med årsrapporten er at give svar på:

- Hvad er status på arbejdet med databeskyttelse i Norddjurs Kommune i 2025?
- Hvilke områder skal vi prioritere i det kommende år?

2025 har været præget af høj aktivitet på både databeskyttelses- og informationssikkerhedsområdet, drevet af interne initiativer og nye eksterne krav. Arbejdet med fortegnelser, Den Gode IT-anskaffelse, konsekvensanalyser, logning samt awareness og e-læring har fyldt betydeligt og viser, at der fortsat er behov for at styrke strukturer, processer og kompetencer.

Der er igen i 2025 opnået gode resultater, blandt andet bedre registrering af sikkerhedshændelser. Samtidig mangler der fortsat fremdrift på centrale områder som ajourføring af fortegnelser og højere gennemførselsprocent på den obligatoriske e-læring.

Erfaringerne fra 2025 samt nye anbefalinger fra Datatilsynet og databeskyttelsesrådgiveren peger derfor på tydelige hovedmål for 2026, herunder styrket databeskyttelsesniveau og forberedelse på kommende regulering som AI-forordningen og NIS2.