rksk.dk

RAPPORT

NATURENS RIGE

Rapport fra databeskyttelsesrådgiveren 2023

Ringkøbing-Skjern Kommune

Indholdsfortegnelse

1. Baggrund 3
2. Fortegnelser 3
3. Awareness 3
4. BDO's arbejde med kontrol af databehandlere 4
5. Internt tilsyn 4
6. Politikker, procedurer, retningslinjer mv. 5
7. Nyt overførselsgrundlag til USA 5
8. Høring fra Datatilsynet om brud omhandlende brug af underdatabehandler i usikkert tredjeland. 5
9. Brud på persondatasikkerheden 6
10. Afgørelse på tilsyn om antal indberettede brud 7
11. ChatGPT og kunstig intelligens 8
12. Afslutning 9

1. Baggrund

Det følger af Databeskyttelsesforordningen art. 38 stk. 3, at databeskyttelsesrådgiveren rapporterer direkte til øverste ledelsesniveau, hvilket i Ringkøbing-Skjern Kommune er Byrådet.

Databeskyttelsesrådgiveren har udarbejdet en rapport årligt siden 2018, da Databeskyttelsesforordningen trådte i kraft.

Det er databeskyttelsesrådgiverens oplevelse, at organisationen i RKSK har taget GDPR til sig og ser GDPR som en naturlig del af kerneopgaven. Det kan dog stadig være svært at indarbejde de nye arbejdsgange, og der kommer løbende nye afgørelser og vejledninger, som kommunen skal forholde sig til. Derfor fylder arbejdet med GDPR meget i de enkelte fag- og stabsområder, det vil blive beskrevet i de følgende afsnit.

2. Fortegnelser

Som beskrevet i tidligere års rapporter skal alle dataansvarlige og databehandlere føre fortegnelser over de behandlingsaktiviteter, de laver i organisationen. Det følger af Databeskyttelsesforordningen art. 30.

De foregående år har Ringkøbing-Skjern Kommune årligt revideret alle fortegnelser over behandlingsaktiviteter.

På baggrund af samarbejdet i KL-Partnerskabet er det besluttet, at Ringkøbing-Skjern Kommune fremover vil gøre brug af resultatet af arbejdet i Partnerskabet, nemlig en skabelon indeholdende 90 behandlingsaktiviteter, som samtidig bliver risikovurderet.

Arbejdet i Ringkøbing-Skjern Kommune om at indføre det nye fortegnelser blev påbegyndt ultimo 2023 og fortsætter i 1. kvartal 2024.

Derfor er der i 2023 ikke sket en revidering af de eksisterende 41 fortegnelser.

3. Awareness

I databeskyttelsesforordningen art. 32 om behandlingssikkerhed er kommunen underlagt krav om at sørge for både tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed. Dette omhandler bl.a. awareness, som skal sikre, at medarbejderne har et passende vidensniveau for at passe på borgernes data.

Arbejdet sker bl.a. ved at udarbejde retningslinjer både centralt og lokalt i fag- og stabsområderne.

Selvom GDPR-kontaktpersonerne var med til at danne beslutningsgrundlaget for, at der ikke skulle være en central styring af awareness i Ringkøbing-Skjern Kommune, valgte alle fag- og stabsområder alligevel at gå sammen om at indkøbe og tage et GDPR-modul i anvendelse. Ansvaret for dette arbejde er decentralt placeret.

Det bliver interessant at følge virkningen af dette tiltag. Vil det være med til at sikre en viden hos alle medarbejdere, der gør, at antallet af brud på persondatasikkerheden falder?

De andre nævnte awareness tiltag i rapporten fra 2022 er tilbagevendende og gælder derfor også for 2023. Det er møder om GDPR, vejledninger mv.

4. BDO's arbejde med kontrol af databehandlere

Som dataansvarlig er kommunen forpligtet jfr. Databeskyttelsesforordningen art. 28 til at sikre, at kommunens databehandlere overholder det aftalte i databehandleraftalerne.

Kommunen har indgået en aftale med Revisionsfirmaet BDO om at føre dette tilsyn på vegne af RKSK. Hvert kvartal fremsendes en rapport fra BDO om de gennemførte tilsyn, hvori der står beskrevet, hvad kommunen bør følge op på i databehandleraftalerne, og med hvilken tilfredshed tilsynet med databehandlerne er udført.

Det er en aftale, som kommunen er meget tilfreds med.

Afledt af arbejdet i KL-Partnerskabet er der nu etableret en kommunal forening om et Fælleskommunalt Databehandler Sekretariat (DBS). Undersøgelser har vist at DBS, med de kriterier de har sat for at føre tilsyn med kommuners databehandlere, endnu ikke kan påtage sig opgaven fuldt ud. I Ringkøbing-Skjern Kommunes tilfælde vil DBS kunne føre tilsyn med ca. 2/3 - altså vil der være en rest på 1/3, som kommunen selv ville skulle føre tilsyn med. Dette er en opgave, som kommunen ikke har hverken ressourcer eller kompetencer til.

Derfor fortsætter samarbejdet med BDO indtil videre. Der holdes øje med udviklingen hos DBS, da det er et godt tiltag at kommunerne går sammen om opgaven.

5. Internt tilsyn

I henhold til de opgaver, databeskyttelsesrådgiveren er pålagt jfr. Databeskyttelsesforordningen art. 39, er overvågning af overholdelsen af Databeskyttelsesforordningen en af disse.

Dette kan bl.a. ske ved internt tilsyn.

I 2023 blev det interne tilsyn gennemført ved bl.a. kontrol med awareness i kommunen baseret på de awareness planer alle fag- og stabsområder havde udarbejdet.

Det var et skriftligt tilsyn, der tog udgangspunkt i for det første at føre kontrol med om tiltagene i awareness planerne var blevet gennemført sammenholdt med eventuelle opmærksomhedspunkter hos de enkelte fag- og stabsområder.

Et af principperne i Databeskyttelsesforordningen er opbevaringsbegrænsning. Det betyder, at man ikke må opbevare personoplysninger i længere tid, end det er nødvendigt for behandlingen. Det har ikke, før Databeskyttelsesforordningens ikrafttræden i 2018, været kutyme, at kommuner har slettet data – tværtimod. Datatilsynet har kørt et tilsyn hos en anden kommune, hvor de har haft fokus på sletning. Afgørelsen var, at denne kommune ikke havde procedurer for sletning og heller ikke havde praktiseret sletning. Kommunen fik et påbud om at få udarbejdet sådanne procedurer og få slettet overflødige personoplysninger i systemerne inden for 3 måneder.

Derfor har det været et fokusområde for DPO'en.

Det var derfor også en del af det interne tilsyn at fag- og stabsområderne skulle fremsende deres egne procedurer for sletning samt dokumentation for udførelse af sletning.

Når kommunen behandler personoplysninger og man i sin risikovurdering har fundet, at der er en stor risiko for borgerne, behandlingen omfatter udsatte eller sårbare personer eller man tager ny teknologi i brug, skal der udarbejdes en konsekvensanalyse, således at kommunen kan få et overblik over, hvilke tiltag der vil kunne nedbringe risikoen eller sandsynligheden for at risiciene vil indtræffe.

Et tredje punkt i det interne tilsyn var derfor at få et overblik over, hvilke konsekvensanalyser, der er udarbejdet i kommunen.

Resultatet af tilsynet var tilfredsstillende i forhold til at gennemføre awareness aktiviteterne.

I forhold til procedurer for sletning og udarbejdelse af konsekvensanalyser, er dette mangelfuldt og der vil blive sat fokus på disse opgaver i 2024.

6. Politikker, procedurer, retningslinjer mv.

Alle politikker, procedurer, retningslinjer mv. udarbejdes eller revideres løbende for at leve op til lovgivning og efterspørgsel.

Følgende er enten udarbejdet eller revideret i 2023, således at krav til persondatasikkerhed er omfattet og alle er godkendt af eller informeret til Udvalget for informationssikkerhed.

- Retningslinjer for konsekvensanalyser (DPIA)
- Procedure for stikprøver i logs
- RKSK Password politik

7. Nyt overførselsgrundlag til USA

Som forklaret i de tre forrige rapporter har der været store vanskeligheder ved at gøre brug af databehandlere og underdatabehandlere fra især USA, hvorfra størstedelen af Cloud udbydere har hovedsæde.

I juli 2023 kom der et nyt overførselsgrundlag vedtaget af EU-Kommissionen. Overførselsgrundlaget hedder Data Privacy Framework (DPF). Det er en selvcertificeringsordning, hvor virksomheder i USA ved at certificere sig, tilkendegiver at de vil leve op til ordningen.

Det betyder, at det i dag ikke længere er helt så vanskeligt at gøre brug af databehandlere og underdatabehandlere i USA. Hvis en amerikansk virksomhed vælger ikke at certificere sig under ordningen, vil der ikke være ændringer i den måde, det skal håndteres på som de sidste 3 år. Man vil så skulle gøre brug af et andet overførselsgrundlag og der vil så også være et større undersøgelsesarbejde, der skal ske samtidig med at der skal indføres supplerende juridiske, tekniske og organisatoriske foranstaltninger.

8. Høring fra Datatilsynet om brud omhandlende brug af underdatabehandler i usikkert tredjeland

I september 2021 indberettede RKSK et brud til Datatilsynet. Bruddet omhandlede en databehandler (leverandør), der gjorde brug af en underdatabehandler i USA, som er et usikkert tredjeland, som EU Kommissionen har afgjort ikke er i overensstemmelse med GDPR. Denne brug af underdatabehandler er sket uden kommunens viden og bliver opdaget ved et tilfælde.

Efter at Datatilsynet har behandlet indberetningen har det givet anledning til uddybende spørgsmål, som af kommunen blev besvaret i oktober 2021. Denne besvarelse gav Datatilsynet anledning til at sende en høring til RKSK, hvor kommunen skulle redegøre for flere ting. Denne høring blev besvaret i maj 2022.

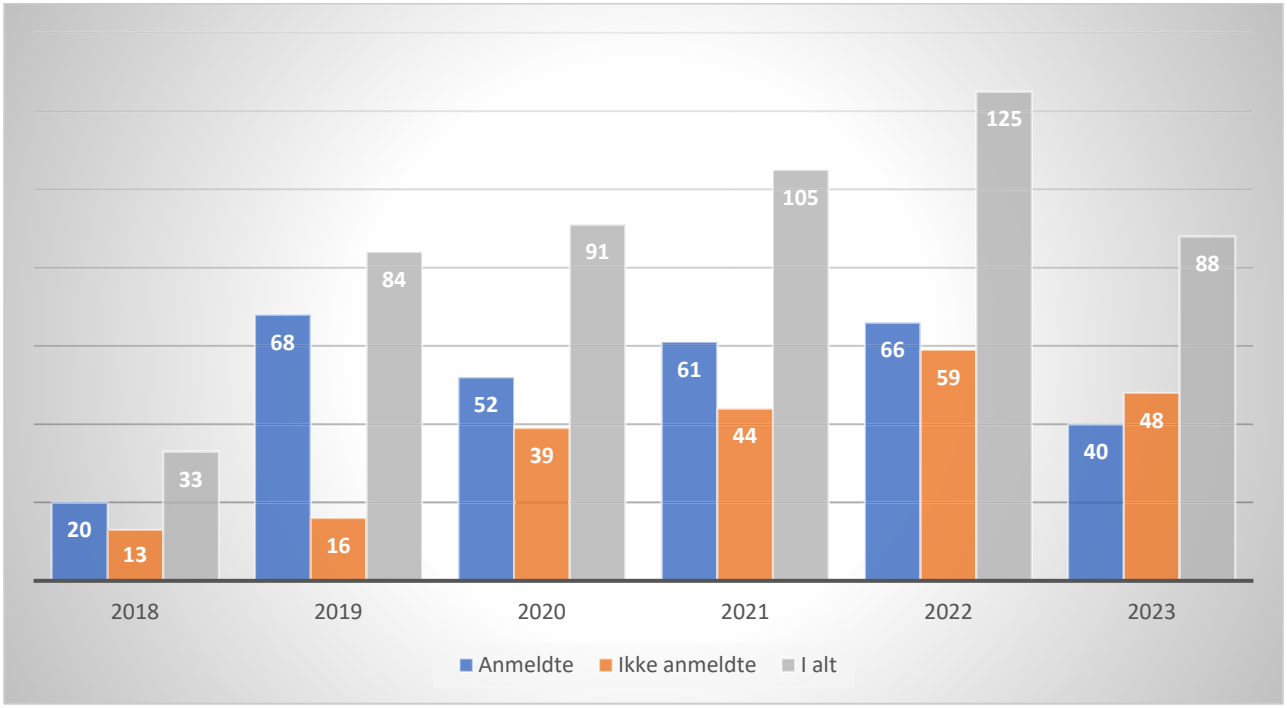
I juni 2023 kom afgørelsen fra Datatilsynet og de vil ikke foretage sig yderligere overfor Ringkøbing-Skjern Kommune.

9. Brud på persondatasikkerheden

I forordningen art. 33 er anført, at den dataansvarlige skal anmelde alle brud til Datatilsynet, hvor der er en risiko for de registreredes rettigheder eller frihedsrettigheder. Denne anmeldelse skal ske inden for 72 timer.

Derudover skal de dataansvarlige registrere alle brud i en hændelseslog, også dem hvor det er vurderet, at det vil være usandsynligt, at bruddet vil udgøre en risiko for den registrerede og dermed ikke bliver anmeldt til Datatilsynet.

Herunder er indsat en tabel, der viser antallet af databrud for Ringkøbing-Skjern Kommune siden forordningen trådte i kraft den 25. maj 2018 og hvorvidt de er blevet anmeldt til Datatilsynet eller ej.



Som det fremgår af diagrammet herover, så har tendensen været støt stigende fra 2018 frem til 2022, hvorefter kurven er knækket. Der har i tidligere år været en bekymring om, hvorvidt det stigende antal af brud havde at gøre med, at Ringkøbing-Skjern Kommune havde flere brud end andre kommuner.

Den awareness der har været i organisationen på personalemøder samt opfølgning på brud - og måske også ved gennemførelse af det tidligere omtalte GDPR.-awarenessmodul - ses nu afspejlet i tallene herover. Det er DPO'ens forhåbning, at kurven forbliver for nedadgående fremover.

Det skal også bemærkes, at ingen af de indberettede brud i 2023 har haft en karakter, hvor det har udgjort en stor risiko for borgerne. Det har typisk været brud, som er sket som følge af menneskelige fejl, og hvert brud har omfattet én eller få borgere.

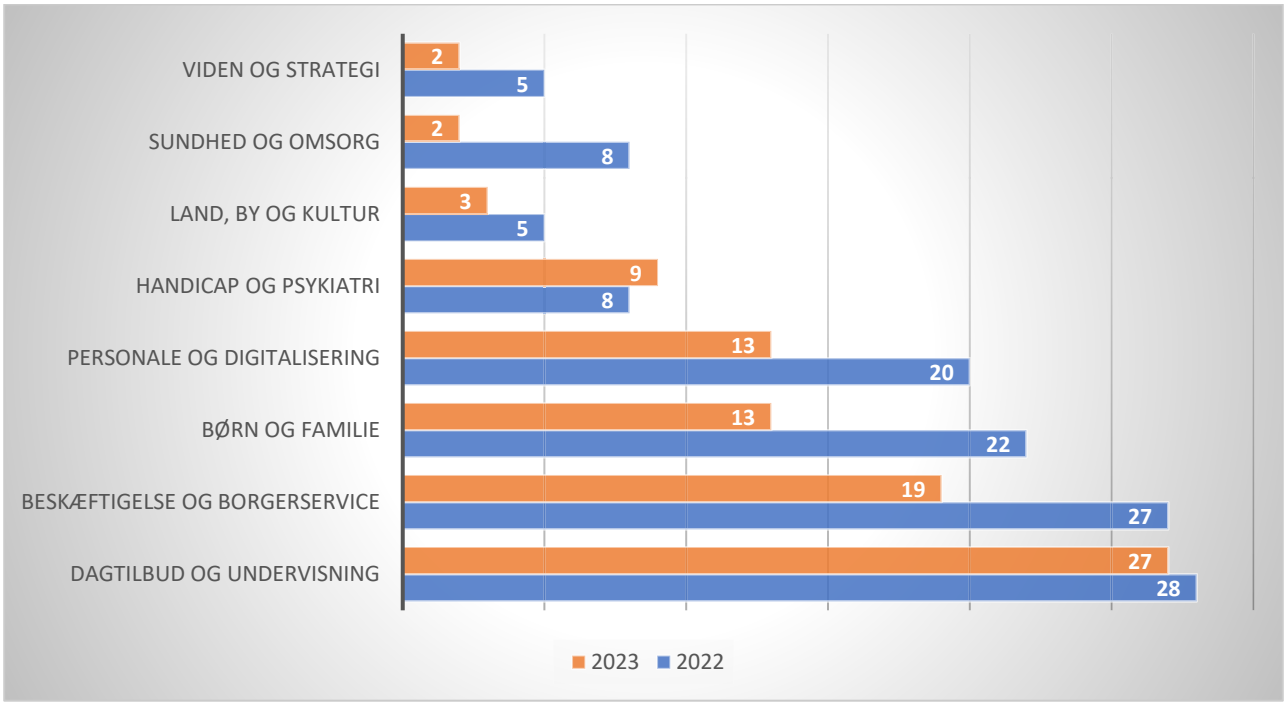
De typiske årsager til brud, der bliver indberettet er:

- Fremsendelse til forkert modtager
- Utilsigtet videregivelse

De typiske årsager til brud, der **ikke** bliver indberettet er:

- Mail sendt usikkert, men viste sig af være krypteret alligevel
- Fremsendelse til forkert intern modtager

Fordelingen af brud i henholdsvis 2022 og 2023 pr. fag- og stabsområde:



10. Afgørelse på tilsyn om antal indberettede brud

Som beskrevet i rapporten for 2021, så har Datatilsynet gennemført tilsyn med flere kommuner – både de kommuner, som har flest indberettede brud pr. indbygger, og de kommuner som har færrest. For at se indholdet af tilsynet, anbefales det at læse rapporten fra 2021.

Ringkøbing-Skjern Kommune blev udvalgt, da kommunen har væsentlig flere indberettede brud pr. indbygger end andre kommuner.

Tilsynet foregik i sommeren 2021 og i august 2023 blev det afsluttet.

Datatilsynet fandt på baggrund af Ringkøbing-Skjern Kommunes besvarelse af tilsynet, at kommunen havde truffet passende sikkerhedsforanstaltninger med henblik på at nedbringe antallet af brud.

Datatilsynet kunne konstatere et fald i antallet af indberettede brud i tiden efter tilsynet.

Datatilsynet skrev dog følgende:
"Idet der imidlertid fortsat anmeldes en del brud på persondatasikkerheden, hvor der er sket uautoriseret videregivelse af personoplysninger, henstiller Datatilsynet til, at kommunen fortsat, løbende har fokus på at gennemføre uddannelses- og awarenessaktiviteter mv. samt at sikre, og at procedurer, retningslinjer, arbejdsgange, tekniske sikkerhedsforanstaltninger mv. løbende opdateres eller indføres, herunder som følge af konstaterede brud på persondatasikkerheden."

Det er ligeledes DPO'ens anbefaling at fortsætte med de nuværende kriterier for anmeldelser af databrud til Datatilsynet, samtidig med at der bevares det gode fokus på både de organisatoriske og tekniske foranstaltninger for at nedbringe antallet af brud yderligere.

11. ChatGPT og kunstig intelligens

Det går stærkt inden for kunstig intelligens. I november 2022 kom den første udgave af ChatGPT og siden har ingen set sig tilbage. Det har været og er stadig et stort fokusområde for Ringkøbing-Skjern Kommune og der er udarbejdet retningslinjer for brugen af netop generativ AI herunder bl.a. ChatGPT. Af disse fremgår det bl.a. at personoplysninger ikke må deles i ChatGPT.

Kunstig intelligens (AI) vinder også frem på andre områder og her bliver det hurtigt sværere at arbejde med rigtige data i disse løsninger.

Københavns Kommune har forespurgt Datatilsynet om muligheden for dette scenarie:

Københavns Kommune ønsker at udvikle, idriftsætte og gentræne en AI-løsning med udgangspunkt i egne data, der stammer fra historiske sager om tilbud af træning og rehabiliterende indsats. AI-løsningen er tiltænkt som beslutningsstøtte til sagsbehandlere i kommunens sundheds- og omsorgsforvaltning og vil på baggrund af en statistisk analyse med relativt stor nøjagtighed identificere, hvilke borgere der kan gennemføre et træningsforløb, og hvem der vil få effekt af forløbet.

Datatilsynet udtaler, at kommuner vil kunne udvikle og træne en AI løsning efter forordningen, men at drift af en AI løsning skal være hjemlet i national lovgivning, hvilket endnu ikke er en realitet.

Hele udtalelsen fra Datatilsynet kan ses her

Datatilsynet har desuden udarbejdet en vejledning til offentlige myndigheders brug af kunstig intelligens.

Ringkøbing-Skjern Kommune har endnu ikke idriftsat en kunstig intelligens løsning, men DPO'en har kendskab til, at der arbejdes med flere mulige løsninger. Det er her vigtigt at bemærke, at hvis DPO'en skal have en mulighed for at rådgive ordentligt, skal organisationen sørge for at inddrage DPO'en tidligt i processen.

Desuden er kommunen langt fremme med arbejdet med automatisering (robotløsninger). Dette er dog ikke omfattet af kunstig intelligens og dermed heller ikke de strikse regler.

12. Afslutning

Som det fremgår af denne rapport, så arbejdes der stadig, og med stor omhyggelighed i organisationen på, at få GDPR ind i en travl arbejdsdag. Det er databeskyttelsesrådgiverens oplevelse, at alle gerne vil gøre sit bedste for at passe på borgernes personoplysninger – vi låner dem bare!

Datatilsynet har netop offentliggjort deres fokusområder for tilsyn for 2024 og af den liste, er der flere fokusområder som omhandler kommunerne. Bl.a. har Datatilsynet de sidste par år lavet en modenhedsanalyse i nogle kommuner. Af planen for 2024 fremgår det, at de kommuner som ikke tidligere har været omfattet af dette tilsyn, vil blive det i 2024. Ringkøbing-Skjern Kommune har ikke tidligere været omfattet af dette tilsyn, så det forventes at ske. Af dette tilsyn fremgår det også, at der vil være fokus på bl.a. kryptering af harddiske som, ved mangel på kryptering, de senere år har udløst bøder til flere kommuner. Det har Ringkøbing-Skjern Kommune styr på. Derudover vil der også være et fokus på konsekvensanalyser, hvilket også var en del af DPO'ens interne tilsyn i 2023 og på den baggrund vil være et fokusområde i kommunen i 2024.

Det er DPO'ens opfattelse at ingen kommuner er 100% compliance i forhold til GDPR – alle har fokus på meget, men ingen kan have fokus på alt. Dette gælder også for Ringkøbing-Skjern Kommune.

Der skal derfor en vedvarende indsats til at sikre et passende sikkerhedsniveau, således at borgerne trygt kan regne med, at deres personoplysninger behandles korrekt. Det betyder, at GDPR er blevet en reel opgave for hele organisationen, som medvirker til et øget pres på hverdagen i fag- og stabsområderne, men det er en nødvendig opgave at afsætte tid og ressourcer til, for at overholde lovgivningen og sikre beskyttelse af borgernes data.

Ringkøbing, den 18. januar 2024

Jette Rask

Databeskyttelsesrådgiver