RAPPORT

NATURENS RIGE

Rapport fra databeskyttelsesrådgiveren 2022

Ringkøbing-Skjern Kommune

Indholdsfortegnelse

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.

I de sidste to rapporter er det beskrevet, at det grundet Corona-hjemsendelser har været svært at mødes fysisk til møder mv. I 2022 var det kun i januar, at kommunens medarbejdere arbejdede hjemmefra. Det har derfor næsten været et almindeligt år angående arbejdet med GDPR (Databeskyttelsesforordningen).

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 har i organisationen. Det følger af Databeskyttelsesforordningen art. 30.

Ringkøbing-Skjern Kommune gennemfører årligt en revidering af, at alle behandlingsaktiviteter er beskrevet i de fortegnelser kommunen har.

På nuværende tidspunkt har kommunen 41 fortegnelser, som er listet op herunder:

Myndighedsopgaver, service og tilbud til voksne handicappede og sindslidende	Ledelsesinformation Handicap og Psykiatri
Lær at tackle (kurser i Sundhed og Omsorg)	Friplejehjem
Myndighedsudøvelse i Sundhed og Omsorg	Kommunal madservice
Genbrugshjælpemidler	Kommunal pleje, behandling og omsorg
PPR	Familiecentret
Socialrådgivningen	Sundhedsplejen
Tandplejen	Havne
Vej og Park	Genbrugsområdet
Kulturskolen	Udlejning af kommunale ejendomme
Biblioteker	Håndtering af matrikler
Kultur- og Fritidsområdet	Skoleområdet
Administrationen (Dagtilbud og Undervisning)	Daginstitutionsområdet
Kontante ydelser	Flygtningen og integration
Beskæftigelse	Borgerlige forhold
Opux Lex Helbredstillæg	Økonomi
Analyse og Effekt	Forsikring
Ekstern Udvikling	Politisk Administrativt Sekretariat – PAS
Udbud	Jura
GIS	Valg

Løn- og Personaleadministration – selvejende institutioner	Løn- og Personaleadministration
Løn- og Personaleadministration – eksterne enheder	

3. KL-Partnerskabet

Som beskrevet i rapporten for 2021 (Rapporten blev præsenteret for Byrådet den 8. februar 2022) har KL sammen med 43 kommuner arbejdet med flere fælles initiativer om GDPR og Informationssikkerhed.

I rapporten for 2021 beskrives de initiativer, der var gennemført i KL-Partnerskabet i 2021. Der var nogle få initiativer, som først blev gennemført i 2022. De gennemgås I det følgende.

KL-Partnerskabet har sammen med MOCH, som er et firma, der leverer e-Learning, udarbejdet et modul om Forvaltnings- og Offentlighedsloven. Viden og Strategi (Jura) har sammen med organisationen set dette modul igennem. De har vurderet, at Schultz Campus er en bedre løsning og en løsning som Beskæftigelse i forvejen har investeret i . Viden og Strategi arbejder videre med at tilrettelægge en proces for at få det implementeret.

Initiativet om beredskab ift. cyberangreb blev også gennemført i 2022. Her deltog kommunens informationssikkerhedskoordinator. RKSK har igennem flere år arbejdet med beredskabsplaner og gennemførelse af tests af disse. Derfor bidrog RKSK mest med input til udformning af materiale i dette initiativ. RKSK har implementeret det nødvendige omkring beredskab ift. cyberangreb.

Det sidste initiativ var om dokumentationskravet i GDPR. Her deltog databeskyttelsesrådgiveren. Resultatet af dette initiativ var en oversigt over alle artikler i forordningen, hvor der for hver artikel er opført, hvordan dokumentationskravet kan opfyldes. Datatilsynet har ikke villet blåstemple resultatet, hvilket giver en vis usikkerhed om, hvorvidt noget er for vidtgående eller noget andet er utilstrækkeligt. RKSK har valgt at gå med mindst mulig dokumentation inden for rammerne af forordningen.

KL-Partnerskabet er nu lukket ned igen og materialet fra de forskellige initiativer kan ses på https://videncenter.kl.dk

4. 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.

Som nævnt i rapporten fra 2021 blev det besluttet, at der ikke skulle være et centralt awareness system til GDPR. Ansvaret for dokumentation af gennemført awareness ligger decentralt hos de enkelte fag- og stabsområder.

Det har dog siden vist sig, at særligt ét system har udmærket sig ved at lave moduler målrettet bestemte medarbejdergrupper i kommunen. Det har flere fag- og stabsområder nu enten taget i brug eller overvejer at gøre det.

Af andre awareness tiltag kan nævnes at gruppen med GDPR-kontaktpersoner, databeskyttelsesrådgiveren, informationssikkerhedskoordinatoren og den øverste informationssikkerhedsansvarlige holder statusmøder 2 gange årligt, hvor nye opmærksomhedspunkter bl.a. drøftes og igangsættes. Derudover mødes GDPR-kontaktpersonerne og databeskyttelsesrådgiveren til 2 halvdags arbejdsmøder årligt.

På kommunens intranet Forum er der et samarbejdsrum, hvor GDPR-kontaktpersonerne er medlemmer. I denne gruppe sker der gensidig orientering om nye tiltag som nye vejledninger fra Datatilsynet, eller særlige opmærksomhedspunkter som fishingmails, kurser mv.

Databeskyttelsesrådgiveren orienterer løbende på Forum om GDPR. Det kan f.eks. være gode råd om sikkerhed ved hjemmearbejde, revidering af diverse vejledninger/retningslinjer mv.

5. 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 BDO fører 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 indtil videre er meget tilfreds med.

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 2021, således at krav til persondatasikkerhed er omfattet og alle er godkendt af eller informeret til Udvalget for informationssikkerhed.

- Informations- og kommunikationspolitik
- Procedure vedr. kontrol af adgange
- Procedure for stikprøver i logs
- Procedure for offentliggørelse af billeder
- Procedure ved brud på persondatasikkerheden
- Retningslinjer for anvendelse af fjernstyringsværktøj
- Retningslinjer for offentliggørelse af billeder
- Retningslinjer for TR's brug af kommunens it-systemer
- IT Sikkerhedsregler

7. 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 interne tilsyn.

I 2022 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 at føre kontrol med om tiltagene i awareness planerne var blevet gennemført sammenholdt med eventuelle opmærksomhedspunkter hos de enkelte fag- og stabsområder.

Resultatet af tilsynet var, at tiltagene var gennemført i stort set hele kommunen og på tilfredsstillende vis. De få bemærkninger databeskyttelsesrådgiveren havde, blev der efterspurgt en plan for håndtering af. Alle havde håndteret bemærkningerne med det samme og databeskyttelsesrådgiveren modtog derfor ingen planer.

Der blev også gennemført et internt tilsyn med fortegnelser af behandlingsaktiviteter. Her blev der som i 2021 spurgt ind til, om de eksisterende fortegnelser var ajourført og retvisende, om områderne er påbegyndt nye behandlingsaktiviteter, som er omfattet af art. 30 fortegnelseskravet, og om der er udarbejdet fortegnelser på de behandlingsaktiviteter, hvor kommunen er databehandler for en anden dataansvarlig mv.

8. Overførsler af personoplysninger til 3. lande

Som forklaret i rapporten fra både 2020 og 2021 er der store vanskeligheder ved at lave aftaler med leverandører (databehandlere) i usikre tredjelande bl.a. USA, som leverer 80% af verdens cloud løsninger.

I oktober 2022 udstedte Joe Biden et dekret om udveksling af personoplysninger mellem EU og USA. Det er et skridt på vejen men er i sig selv ikke nok til, at vi i EU lovligt kan overføre data til USA. Det skal EU Kommissionen nu tage stilling til, og det forventes, at det sker inden sommeren 2023.

Indtil der foreligger en afgørelse fra EU Kommissionen om, at de har godkendt USA som et sikkert tredjeland, skal kommunen altså følge de anbefalinger og vejledninger, der er kommet fra Det Europæiske Databeskyttelsesråd (EDPB).

9. 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.

Der foreligger endnu ingen afgørelse på dette brud.

10. 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.

År	**Anmeldte til Datatilsynet**	**Ikke anmeldte til Datatilsynet**	**I alt**
2018	20	13	33
2019	68	16	84
2020	52	39	91
2021	61	44	105
2022	66	59	125

Som det fremgår af tabellen herover, så stiger antallet af registrerede brud i RKSK. Det er stadig databeskyttelsesrådgiverens indtryk, at det ikke er fordi kommunen har flere brud end de foregående år – men opmærksomheden er blevet større på at sige til, når der sker fejl. Organisationen tager hånd om disse brud – det bliver italesat på personalemøder, og der skabes awareness om bruddenes karakter, så der kan drages læring af det.

Det skal også bemærkes at ingen af de indberettede brud har en karakter, hvor det har udgjort en stor risiko for borgerne. Det er typisk 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 2022 pr. fag- og stabsområde:

Dagtilbud og Undervisning	28
Beskæftigelse og Borgerservice	27
Børn og Familie	22
Personale og Digitalisering	20
Handicap og Psykiatri	8
Sundhed og Omsorg	8
Land, By og Kultur	5
Viden og Strategi	5

I rapporten fra 2021 fremgik det, at Børn og Familie skilte sig ud fra de andre fag- og stabsområder med væsentlig flere brud, da de var ansvarlige for over 40 % af alle brud i kommunen.

Børn og Familie har arbejdet hårdt på at nedbringe antallet af brud bl.a. ved at lave særlige handleplaner og det er lykkes for dem. Der vil derfor ikke længere være et særligt fokus på dette fagområde.

11. Afgørelse på tilsyn om antal indberettede brud foreligger endnu ikke

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 – se tidligere link under pkt. 3.

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

Tilsynet foregik i sommeren 2021, men der foreligger endnu ikke en afgørelse.

Selvom RKSK blev udvalgt til tilsynet pga. mange indberettede brud, vil databeskyttelsesrådgiveren ikke råde kommunen til at ændre praksis på området, før der foreligger en afgørelse fra Datatilsynet.

Det forlyder også, at der er en revideret vejledning om håndtering af brud på vej fra Datatilsynet.

12. Pressens bevågenhed

Der har også i 2022 været en interesse fra pressens side på, hvordan kommunerne håndterer brud på persondatasikkerheden.

I november var der bl.a. et indslag i TV-avisen om hvilke typer af brud, kommunerne laver, og hvilke konsekvenser det kan have for borgerne.

Jyllands Posten har søgt aktindsigt hos Datatilsynet og der fundet ud af, at RKSK ligger højt på landsplan over antallet af indberettede brud. Jyllands Posten har bl.a. interviewet databeskyttelsesrådgiveren i RKSK og skrevet en artikel i november, hvor kommunen bliver nævnt.

Igen skal det nævnes, at nogle af de eksempler på konsekvenser for borgerne, som både DR og Jyllands Posten er kommet frem med, er langt mere alvorlige end de brud, som er sket i RKSK.

Det er databeskyttelsesrådgiverens indtryk, at kulturen i RKSK om at gøre opmærksom på, når der sker et databrud og samtidig drage læring af det, ser ud til at virke.

13. 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!

Lejre Kommune var den første kommune, der blev idømt en bøde. Bøden lød på 50.000 kr. for manglende behandlingssikkerhed, da der var en praksis om at lægge referater fra møder om børn af særdeles følsom og beskyttelsesværdig karakter på kommunens intranet, som alle medarbejdere har adgang til. Der var ikke logning på intranettet og dermed ikke passende sikkerhed.

Lolland Kommune er indstillet til en bøde på 50.000 kr. for at have udsat borgernes oplysninger for unødig risiko, da medarbejderne kunne slå adgangskoder på telefoner og tablets fra.

Hørsholm Kommune er nu idømt en bøde på 50.000 kr. for ikke at have krypteret harddisken i en stjålet pc.

Som beskrevet er de første sager nu prøvet i retten, hvilket er endt ud i de to beskrevne bøder, mens flere er indstillet til bødestraf.

Med de endnu ikke afsluttede sager, kommunen har ved Datatilsynet, er der en risiko for at kommunen enten får kritik eller bliver indstillet til bøde.

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 11. januar 2023

Jette Rask

Databeskyttelsesrådgiver