Ballerup
Kommune

DPO Rapport – 2022

Indhold

Indledning

Denne rapport er udarbejdet med henblik på, at give kommunens øverste ledelse en status på Ballerup kommunes arbejdet med og overholdelse af de databeskyttelsesretlige regler - som fastlagt i EU-Databeskyttelsesforordningen (GDPR) (EU 2016/679), samt i de danske vedtagne bestemmelser om samme (Databeskyttelsesloven nr. 502 af 23/05/2018).

DPO (databeskyttelsesrådgiver) funktionen har til opgave at rådgive kommunens ledelse og medarbejdere om GDPR. Der føres tilsyn med, at forvaltningen efterlever databeskyttelsesreglerne på betryggende vis og står til rådighed for sparring med organisationen. Der gennemføres en række planlagte kontrolaktiviteter i løbet af året, mens der også er plads til at se på ad hoc eller fritstående aktiviteter, som udvælges på baggrund af aktualitet og risiko i forhold til den registrerede. DPO'en er kommunens uvildig rådgiver ud i GDPR spørgsmål. De overordnede rammer for DPO'ens opgaver beskrives i databeskyttelsesforordningens artikel 39.

DPO-funktionen i Ballerup Kommune deles med de tre andre kommuner i IT-F fællesskabet. Fællesskabet arbejder på at styrke GDPR-samarbejdet omkring de fire kommuner. DPO'en faciliterer et GDPR-netværk, som giver mulighed for sparring og udveksling af erfaringer mellem de GDPR ansvarlige, samt undersøge muligheden for at formaliseret et samarbejde på udvalgte områder.

Rapporten indeholde ud over en status på kommunens arbejde med GDPR en række anbefalinger til det videre arbejde. Ligeledes omtales kort DPO'ens kommende tilsyns-tematikker.

Metode

Årsrapporten beskriver overordnet kommunens arbejde med databeskyttelse og informationssikkerhed. Indholdet bygger på DPO'ens observationer, ugentlig møde med GDPR teamet, planlagte tilsyn samt aktuelle problemstillinger.

Sammenfatning og anbefalinger

Overordnet har kommunen styr på rammerne for databeskyttelse, og der arbejdes med stor omhyggelighed i organisationen på at få GDPR ind i en travl arbejdsdag.
Der vil formentligt være et udviklingspotentiale i mange år fremover, da databeskyttelse fortsat udvikler sig. Derfor anbefales det, at der fortsat er fokus på, at området har nødvendige ressourcer, bakket op af et ledelsesmæssigt fokus. Erfaringen viser, at en vedvarende forankring af

GDPR ud i organisationen ofte lykkedes bedre, når ledelsen har fokus op at prioritere indsatsen.

Det er DPO'ens anbefaling, at der i 2023 er ekstra fokus på følgende områder:

- Risikovurderinger over behandlingsaktiviteter og IT-systemer
- Fortegnelser – opfølgning som en del af årshjulet
- Fortsatte ressourcer til GDPR- og informationssikkerhedsopgaven
- Awarenes og kommunikation om GDPR i hele organisationen
- IT-Forsyningens GDPR compliance som databehandler (modenhedsanalysens)

DPO'ens arbejde

Gennem 2022 har der på ugentlig basis været afholdt statusmøder med god dialog om store og små GDPR dagsordener. En praksis der giver tid til fordybelse og indsigt i dagligdagens arbejde med GDPR i kommune. Det giver samtidig mulighed for at agere hurtigt på nye problemstillinger, afgørelser og udviklingen generelt.

Rådgivning i forbindelse med databehandleraftaler fylder stadig en del, da det til stadighed er udfordrende fx at få klarhed over databehandlerkonstruktionen og de iboende risici.

Google-sagen (brug af GWfE på skoleområdet), brug af US cloud løsninger ex. Aulas brug af AWS (Amazon Web Service) og EU's nye overførselsgrundlag til usikre tredjelande afventer stadig afklaring, og giver anledning til forvirring og mange spørgsmål i forvaltningen. Udviklingen følges intenst så kommunen hurtigt kan reagere, når der kommer en afklaring på disse problemstillinger.

Ud over GDPR teamet har også andre dele af forvaltningen, trukket på DPO rådgivning i mange forskellige spørgsmål. Fx brug af samtykke, hjemmel til behandling af en speciel type personoplysninger, samarbejde med forskningsinstitutioner mm.
På især skoleområdet, har der været mange GDPR-mæssige udfordringer, og vi har være i løbende dialog med C-SIK/skoleområdet. GDPR teamet inddrages altid i spørgsmålene til DPO'en, for at sikre at viden forankres i organisationen.

Der er etableret en GDPR netværk på tværs af de 4 IT-F kommuner. Der har været afholdt en række møder, med en dagsorden der bestemmes af kommunerne og DPO'en i fællesskab. Aktuelle sager og tematikker drøftes og erfaringer udveksles. DPO'en fungere som facilitator på møderne.

Antallet af borgerhenvendelser har ikke været mange, og dem der har været, har for det meste drejet sig andet end GDPR, typisk utilfredshed med afgørelse i en sag eller dårlig kommunikation. Disse henvendelser er formidlet videre til rette instanser-

Tilsyn (planlagte)

Der er gennemført 6 (på forhånd planlagte) tilsyn i 2022:

	1. Sikkerhedsbrud	**2. Sikkerhedsbrud**	**3. Risikovurdering** – behandlings-processer
(hjælpe Tilsyn	En stor del af GDPR compliancearbejdet handler om korrekt håndtering og dokumentation af brud på persondatasikkerheden. Der er gennemført tilsyn med regler, procedurer og foranstaltninger på området.	Med udgangspunkt i en oversigt over sikkerhedsbrud og hændelser for 2021 og 2022, har vi gennemgået de typer sikkerhedsbrud og -hændelser Ballerup kommune har haft. Spørgsmål: Hvilken type hændelser går igen? Er der et mønster? Hvad har i gjort for det ikke sker igen? Hvad kunne man gøre for at undgå/ minimere fejlene?	Sikkerhed er et af de grundlæggende principper for behandling af personoplysninger. De sikkerhedsforanstaltninger, som skal iværksættes, skal vælges og beskrives på baggrund af risikovurderinger. Er der gennemført risikovurdering for alle kommunens IT-systemer som behandler personoplysninger? Følges der struktureret op på risikovurderingerne?
Resultatet	Efter gennemgang af skriftlige procedurer og retningslinjer for indberetning af sikkerhedsbrud, indberetningsformular, log over sikkerhedsbrud, ansvarsfordeling, awareness aktiviteter mv., må det konstateres at det ikke giver anledning til anmærkninger eller ydereligere kommentarer.	Langt de fleste sikkerhedsbrud skyldes menneskelige fejl – en gennemgående tendens på landsplan. I håndteringen af indmeldelser, spørges altid ind til hvorledes anmelder af sikkerhedsbruddet, vil sikre det ikke sker igen. Men der sker ikke en systematisk opfølgning efter hændelsernes afslutning.	Ballerup har en risikobaseret tilgang til vurdering af behandlings-aktiviteter. Det er helt legitimt. På en række områder er der gennem-ført en vurdering af risikoen for den registrerede, men der er et udestående. Der foreligger ikke en samlet plan for gennemførelse og opfølgning for risiko-vurderinger.
Anbefalet handling	**Anbefaling:** at der fortsat skabes awareness om sikkerhedsbrud og indmeldelse af disse til GDPR teamet. Vi ved af erfaring, at det skærper medarbejdernes opmærksomhed, i det daglige arbejde.	**Anbefaling:** Der bør afsættes tid til opfølgning af sikkerhedsbrud sammen med de pågældende centre, hvor sikkerhedsbruddene er sket. Der bør arbejdes mere målrettet med at skærpe sikkerheden der	**Anbefaling:** Datatilsynet har fokus på sikkerheds- og dokumentations-arbejdet i kommunerne. De krav vi ser, de stiller i Google-sagen og i de afgørelser de træffer, viser at den del af kommunens compliance. er en

		hvor sikkerhedsbrudene sker. Lederne skal klædes på til, at kunne træffe de rette beslutninger, og støtte deres medarbejdere i evt. nye rutiner og sikkerheds-foranstaltninger.	forudsætning for al aktivitet. Derfor bør kommunen prioritere at få gennemført risikovurderinger og skabt en struktureret tilgang til sikkerheds- og dokumentations-arbejdet.

	4. Tredjelands-overførsler	5. Slettefrister	6. Arkivering
(hjælpe) Tilsyn	I Datatilsynets cloud-vejledning fra 2021, anbefales det, at kommunen har overblik og it-løsninger og overførsler til 3. lande. Datatilsynet forventer at overblik er etableret, supplerende for-anstaltninger gennem-ført og at der løbende bliver fulgt op på overførslerne.	Med udgangspunkt i en konkret observation i en af kommunerne, gav det anledning til at se på kommunens håndtering og dokumentation af slettefrister i personalesager.	Datatilsynet har interesseret sig for kommuners håndtering af arkivalier, herunder specifikt kommunernes overholdelse af de særlige regler om adgang til arkivalier inden tilgængelighedsfristernes udløb.
Resultatet	På undersøgelsestids-punktet lå en komplet liste over it-systemer inkl. evt. overførsler til 3. lande. Listen indeholder endvidere det aktuelle overførselsgrundlagt.	I Ballerup kommune blev der ikke fundet data der burde være slettet. Men der manglede retningslinjer og dokumentation for sletteprocedure på området.	Arkivering og arbejdet med arkivalier generelt, er der ikke noget GDPR-mæssigt at udsætte på. Reglerne om adgang til arkivalier er kendt, men ikke som sådan dokumenteret skriftligt. Der har ikke været nogen specifikke forespørgsler af denne karakter de seneste mange år. Det har derfor ikke været muligt at afprøve om de uskrevne regler har været mangelfulde. Det antages efter dialog med arkivaren, at en forespørgsel ville være håndteret i overensstemmelse med gældende regler.

Anbefalet handling	**Anbefaling:** Der sker konstant ændringer i udviklingen på området. Opfølgning anbefales at være en del af GDPR teamets årshjul.	**Anbefaling:** At få udarbejdet retningslinjer og anden dokumentation for sletning af personalesager samt en procedure for at sikre det overholdes fremover. Jeg er vidende om at arbejdet med dette ER påbegyndt og godt i gang.	**Anbefaling:** At der udarbejdes skriftlige procedure for hvorledes reglerne håndteres.

Sammenfattende for de gennemførte tilsyn, må konkluderes at kommunen er godt med i forhold til at efterleve GDPR.
Risikovurderinger er et udestående, som det anbefales at få prioriteret. Der er meget fokus på netop risikovurderinger og evt. tilhørende konsekvensanalyser, og mangel her på, kan føre til kritik eller andre sanktioner fra Datatilsynet.

Andre observationer

Databeskyttelse og ressourcer
Databeskyttelsesretten udvikler sig i disse år med stor hastighed, og mange også mere grundlæggende spørgsmål er fortsat under afklaring. Frekvensen af afgørelser fra tilsynsmyndigheder, domstole og EU Domstolen er høj, og vejledninger fra både de nationale tilsynsmyndigheder og i særdeleshed EDPB (Det Europæiske Databeskyttelsesråd) tilfører hele tiden nye bidrag til forståelsen og fortolkningen af reglerne. Det betyder fortsat at området er under stadig forandring, hvilket medfører en kontinuerlig strøm af (ekstra) arbejde til de dataansvarlige (kommunen) og ikke mindst de GDPR ansvarlige.

Generelt har 2022 været præget af flere større sager og problemstillinger; Google-sagen, overførelsesgrundlag/3. landsoverførsler bl.a. Aula, compliance i forbindelse med en række fælleskommunale it-løsninger, brug af billeder på skoleområdet for at nævne nogle.
Ens for de fleste af disse sager, er at de har udstillet, hvad den dataansvarlige (kommunen) forventes at kunne dokumentere på et givent område. Reglerne i Databeskyttelsesforordningen er stadig genstand for fortolkning og vurdering, hvilket til stadighed rykker ved tilstrækkelighedskravet i forhold til at være compliant.
Vurderingen er, at kommunerne står over for en (fortsat) stor opgave med at være compliant.
Derfor anbefales det, at der fortsat sikres ressourcer til området, så kommunen kan håndtere de øgede krav til dokumentation og vedligeholdes her af. For at sikre en god forankring i organisationen, er det nødvendigt at også ledelsen er klædt på til at efterleve GDPR. Der er

observeret situationer hvor GDPR teamet bliver mødt af medarbejdere i andre centre, som ikke får den fornødne opbakning fra deres nærmeste leder, til at arbejde med opgaven.

Opfølgning på fortegnelser
Sidste års anbefalinger omfattede bl.a. øget fokus og indsats omkring opdatering af fortegnelser. Ballerup kommune har gjort en stor indsats med fortegnelser, og der foreligger fortegnelser for alle centres. Der er opbygget en struktur og et overblik, som gør det muligt at inddrage organisationen i arbejdet og dermed forankre processen lokalt. Set i lyset af før omtalte øgede krav til dokumentation og detaljegrad, anbefales det at fortsætte de gode takter og indarbejde løbende opfølgning i GDPR temaets årshjul.

Modenhedsanalyse
Datatilsynet førte i efteråret et skriftligt tilsyn med en række kommuner, for at vurdere modenheden inden for databeskyttelser og informationssikkerhed. Formålet med egen-evalueringen var både at give Datatilsynet blik for bestemte emneområder med behov for øget indsats, men også at understøtte en mere forebyggende tilgang.

Ingen af de 4 kommuner i vores kreds blev udpeget til at gennemføre modenhedsanalysen. Men vi benyttede anledningen til gennemgå analysen, for at få en fornemmelse af, om den aktuelle modenhed var i overensstemmelse med min forventning og viden.
Det er min opfattelse at Ballerup kommune og IT-Forsyningen (som driftsoperatør), på en række områder lever op til hvad der forventes, men en gennemgang viste, at ikke al dokumentation herfor er udarbejdet eller tilgængelig. Det bør der følgels op på.

Sammenfattende er Datatilsynets anbefalinger på baggrund af deres analyse, følgende anbefalinger, som stemmer meget godt overens med resultatet af vores egen-evaluering:

- Ledelsen bør aktivt involveres i arbejdet med databeskyttelse og informationssikkerhed, bl.a. ved at sikre at organisationens risikovurderinger, politikker og årshjul er opdaterede og retvisende, og ved at sikre at medarbejderne er tilstrækkeligt trænede i sikker behandling af personoplysninger, samt at organisationen er i stand til at opdage usædvanlig, uhensigtsmæssig eller ulovlig adfærd.
- Skab overblik over behandlingsaktiviteter og de risici for de registrerede, der er forbundet med behandlingsaktiviteterne, og etabler strukturerede arbejdsgange til regelmæssigt at evaluere tiltag inden for databeskyttelse og informationssikkerhed.
- Beskyt adgange til systemer og databaser, hvor der opbevares og behandles personoplysninger med henblik på at opdage uhensigtsmæssig eller ulovlig adfærd.
- Evaluer beskyttelsen af adgange til systemer og databaser, hvor der opbevares og behandles personoplysninger, med henblik på at sikre effektive foranstaltninger.

- Forebyg utilsigtet offentliggørelse og/eller videregivelse af personoplysninger til uvedkommende ved kommunikation, som er den mest udbredte type af sikkerhedsbrud jf. Datatilsynets statistik.
- Afprøv om foranstaltninger er virkningsfulde og effektive, herunder backup og beredskab, som udgør grundlæggende sikkerhed, til at reetablere drift under angreb og til at håndtere hændelser.
- Foretag regelmæssig kontrol med databehandlere.

Det anbefales af disse punkter indarbejdes i det kommende arbejde med GDPR og informationssikkerhed.

Sammenfatning

Det er DPO'ens opfattelse, at Ballerup kommunes arbejder målrettet og struktureret med sit compliance arbejde, der sikrer, at der bliver fulgt op på behandlingsaktiviteter og dokumentation. Overordnet set er der dokumenteret en række processer og tiltag, og det er min vurdering at kommunen generelt behandler borgers og ansattes personoplysninger ansvarlighed.

Der vil formentligt altid være et udviklingspotentiale, da databeskyttelse hele tiden udvikler sig. Derfor bør der være fortsat fokus på, at området har de nødvendige ressourcer og ledelsesmæssige opbakning.

Ballerup har arbejdet med DPOnes anbefalinger fra 2021. Kommunens bør, for at sikre det grundlæggende fundament for kravene i databeskyttelsesforordningen (GDPR), arbejde målrettet med at få gennemført relevante risikovurderinger.

Jeg er vidende om, at arbejdet med risikovurderinger er et fokusområde for 2023.

Sammenfattende er DPO'ens anbefaling, at der i 2023 er ekstra fokus på følgende områder:

• Risikovurderinger over behandlingsaktiviteter og IT-systemer
• Fortsatte ressourcer til GDPR og informationssikkerhedsopgaven
• Awarenes og kommunikation om GDPR i hele organisationen
• Fortegnelser – opfølgning som en del af årshjulet
• IT-Forsyningens GDPR compliance i forhold til temaerne i Modenhedsanalysen.

Indsatsområder for 2023

Indsatsområder for 2023 gennemføres som skriftlige tilsyn. Temaet beskrives i et skriftligt oplæg, som forventes besvaret fra forvaltningen inden for en passende periode. Svarene gennemgås og drøftes på et afsluttende møde mellem DPO og GDPR teamet/andre dele af forvaltningen.

1. Adgangskontrol og logning/stikprøvekontrol – generelt politik og specifikke nedslag bl.a. SAPA
2. SAPA – brugerstrategi, opsætning og adgangskontrol
3. TV-overvågning
4. Behandling af persondata på kommunens hjemmesider.

Malene Rafn Permin
DPO
Juli 2023