BALLERUP KOMMUNE

DPO RAPPORT 2021 (DATABESKYTTELSES-RÅDGIVER)

Status på GDPR arbejdet i Ballerup kommune

Databeskyttelsesrådgiverens (DPO'ens) rapport 2021
Status på GDPR arbejdet i Ballerup Kommune

1. Forord

Denne rapport har til formål at give Ballerup Kommune – ledelse og interesserede medarbejdere - en status på arbejdet med databeskyttelse i kommunen og en opfølgning på den tidligere DPO's observationer. Rapporten indeholde derudover en række anbefalinger til det videre arbejde med GDPR. Som bilag er udarbejdet DPO'ens årshjul 2022 for tilsyn med udvalgte tematikker.

2. Sammenfatning og anbefalinger

Ballerup Kommune arbejder målrettet med GDPR, og der er en god dynamik i GDPR-teamet, som gør at der overordnet er styr på opgaveporteføljen. Opgaverne er imidlertid flere, end hvad der er ressourcer til. Der er yderligere ressourcer på vej til GDPR teamet, som skal styrke arbejdet med databehandlere, men der er et efterslæb, der skal indhentes på store dokumentationsopgaver såsom fortegnelser og risikovurderinger

Det er et godt initiativ, at der er etableret et GDPR-ambassadørnetværk, som kan bidrage til at facilitere nogle af de GDPR-opgaver, der ligger decentralt. Dette er primært opgaver, hvor særlig faglig indsigt i arbejdsgange og systemer er nødvendige for at udarbejde dokumentationen, samt i forbindelse med awareness, oplæring og adfærds-ændringer blandt medarbejderne. Derudover skaber netværket gode rammer for kommunikation og rådgivning vedr. GDPR. Derved frigives ressourcer i GDPR-teamet til andre GDPR opgaver, bl.a. de løbende vedligehold af compliance-porteføljen og store udefra kommende dagsordner som kræver en stor arbejdsindsats. Tilsvarende vil et samarbejde med de tre andre kommuner om nogle af de opgaver, der er ens for kommunerne og pt. ikke bliver prioriteret, kunne reducere nogle af de pukler, der er.

Trods de gode rammer for GDPR og et acceptabelt modenhedsniveau i organisationen, er det vigtigt at fastholde fokus på den gode og tilstrækkelige databeskyttelse i alle behandlingsaktiviteter. Der skal fortsat arbejdes med området. Kombinationen af mere end 5000 medarbejdere med jævnlig udskiftning af personalegruppen, ny teknologi og en travl hverdag for mange, betyder alt andet lige, at der løbende vil være behov for at holde fokus på, hvordan vi behandler persondata i kommunen. Det gælder både i de komplekse problemstillinger, såsom lagring af data i US cloud-løsninger, udvikling af nye IT-løsninger og i forbindelse med de mange tusinde mails med personoplysninger, der sendes til og fra kommunen hver dag. I alle tilfælde er mennesker involveret, hvilket betyder at kommuner generelt er særlig eksponeret for "menneskelige fejl". Derfor ligger der fortsat en vigtig opgave for ledelsen i at minde medarbejder om retningslinjer og god praksis for den korrekte databehandling, der gælder lokalt. Der er igangsat et godt program for awarenes, som bør suppleres af et ledelsesmæssigt fokus.

Indsatsområder (i prioriteret rækkefølge)	**Anbefaling**
Risikovurderinger og konsekvensanalyser (DPIA)	Få udarbejdet risikovurderinger for de behandlingsaktivitet og it-løsninger der indeholder persondata. Det anbefales at der skabes et overblik over, om der mangler at blive udarbejdet konsekvensanalyser (DPIA) på behandlingsaktiviteter og it-løsninger.
Fortegnelser	Fortegnelserne skal opdateres efter de seneste anbefalinger og skabeloner. Det anbefales at der etableres en proces der sikre en løbende vedligeholdelse.

Datasikkerhed – adgangsrettigheder og logning	Det anbefales at der indføres en struktureret og dokumenteret proces for logning it-brugere i kommunens it-systemer der behandler personoplysninger. Datatilsynet anbefaler tilsyn på udvalgte bruger 3-4 gange om året, for systemer der behandler mange følsomme persondata om borgerne
Styring og ansvarsfordeling af GDPR arbejdet samt awarenesskampagner	Skabe endnu bedre ledelsesmæssig forankring af GDPR opgaven. Fokus på ressourcerne i GDPR teamet – de skal svare til mængden af opgaver. Det anbefales at få e-læringsværktøjet op og køre og fortsæt med at være tilstede i organisationen og formidl GDPR på en nærværende måde. Det skal dokumenteres at der er gennemført undervisning/e-læring af alle medarbejdere.
Kryptering, anonymisering /pseudo-nymisering	Det er et generelt opmærksomhedspunkt at arbejde med kryptering, anonymise-ring/pseudonymisering af data ifm. overførsel af data til fx forskningsinstitutioner og anvendelse af US cloudleverandører.

3. DPO'ens funktion

De overordnede rammer for DPO'ens opgaver beskrives i Databeskyttelsesforordningens artikel 39:

- DPO'en har til opgave at underrette og rådgive kommunen og dens ansatte om databeskyttelses-retlige spørgsmål
- DPO'en har til opgave at overvåge overholdelsen af forordningen samt anden EU-ret eller national ret vedrørende databeskyttelse
- DPO'en har til opgave at rådgive vedrørende databeskyttelse, når der foretages Konsekvensanalyse
- DPO'en skal samarbejde med Datatilsynet

DPO-funktionen i Ballerup Kommune deles med de tre andre kommuner i IT-F fællesskabet. Fællesskabet har, udover hvad forordningen forventer af DPO'en, ønsket at DPO'en bidrager til at styrke samarbejdet mellem de fire kommuner, bl.a. ved opbygning af et GDPR-netværk, som giver mulighed for sparring og ud-veksling af erfaringer, samt give input til, hvordan et formaliseret samarbejde om udvalgte områder af GDPR-indsatsen kan udformes (med udgangspunkt i at mange opgaver er identiske for kommunerne).

4. Grundlaget for arbejdet med databeskyttelse i Ballerup

Jeg tiltrådte som Databeskyttelsesrådgiver (DPO) den 1. april 2021. Det har været ni spændende, travle og corona-ramte måneder som DPO for de fire kommuner. Store dele af 2021 er gået med, at opbygge kend-skabet til de fire kommuner, og fordybe mig i hvordan kommunerne hver især arbejder med GDPR. Indblik-ket i Ballerup kommune er temmelig godt efter godt 3 års ansættelse. Ikke desto mindre ser jeg frem til i 2022, at komme mere rundt i centrene og tale om GDPR udfordringer, formidle tendenser, afgørelser fra Datatilsynet og tematikker, som efter min mening er aktuelle og væsentlige for den kommunale verden.

Siden 25. maj 2018, hvor Databeskyttelsesforordningen trådte i kraft, har Ballerup Kommune arbejdet mål-rettet med at sikre nødvendige GDPR-regler, implementering, procedurer og organisering. Arbejdet danner et godt og solidt grundlag for det videre arbejde og dokumentation for håndtering af databeskyttelse.

En forudsætning for at være DPO for fire kommuner er, at hver kommune har en veletableret GDPR funk-tion, som samarbejder tæt med DPO'en, og som kan opbygge en stor faglig viden om GDPR. Det betyder også ekstra pres på ressourcerne. Ballerup Kommunes GDPR-funktion består af én fuldtidsstilling fordelt på to medarbejdere placeret i Afsnit for Digitalisering og Forretningsudvikling i Center for Politik og Organisa-tion. Arbejdet med GDPR i Kommunen er tæt knyttet til arbejdet med IT-sikkerhed. Det er ofte svært at skille de to discipliner ad, og et struktureret samarbejde giver god synergi og udnyttelse af ressourcerne.

For yderligere at styrke de GDPR-ansvarliges viden om GDPR og udveksle erfaringer har jeg etableret et **GDPR-netværk** for de fire kommuner. GDPR-netværket faciliteres af DPO'en. Dagsordenen fastsættes af deltagerene sammen med DPO'en, og vi har allerede gennemført et par vellykkede møder. Forventningerne til 2022 er' at fællesskabet udvides til at udvikle et egentligt samarbejde om centrale GDPR-opgaver, som de fire kommuner har til fælles. Et bud på en sådan fælles opgave er et fælles elektronisk vidensbank til dokumentation, arbejdspapirer, politikker og retningslinjer. Derudover skal det afklares hvorvidt og i så fald hvordan kommunernes GDPR-funktion kan samarbejde om compliance-opgaver såsom fortegnelser, risikovurderinger og det omfattende arbejde med indgåelse af og tilsyn med databehandleraftaler. Der er basis for, at dette vil styrke arbejdet med GDPR i den enkelte kommune, samt udnytte ressourcerne endnu bedre.

5. DPO'ens observationer

5.1 Samarbejdet om GDPR i Ballerup

Overordnet vil jeg fremhæve det gode samarbejde med GDPR-temaet, både fra distancen og som nu, hvor vi har mulighed for at mødes fysisk. Det er tydeligt at GDPR-teamet føler ejerskab over opgaven og forsøger at inddrage hele organisationen i arbejdet med henblik på at få så GDPR ud at leve i alle centre. Mængden af opgaver med at være GDPR-compliant, håndtere sikkerhedsbrud og databehandleraftaler, udarbejde compliance-dokumentation, være ansvarlig for awareness-træning, samt stå til rådighed for medarbejdere og ledere som rådgivere og sparringspartnere er vedvarende meget stor.

Jeg holder faste ugentligt møde med GDPR-temaet med det overordnede formål at blive inddraget, rådspurgt og orienteret om alt væsentligt i arbejdet med GDPR. Derudover holder jeg en gang om måneden statusmøde med chef for Afsnit for Digitalisering og Forretningsudvikling. Jeg tilstræber at være fysisk tilstede hver uge i alle kommunerne, enten i forbindelse med faste møder med Kommunens GDPR-team eller ad hoc møder med organisationen. Det er vigtigt for mig at være fleksibel og være tilstede, når der er brug for det, fremfor at have faste dage i hver kommune.

5.2 Forankring af GDPR i organisationen

I november 2021 etableredes et GDPR-ambassadørnetværk, som har til formål at styrke forankringen af GDPR- i enkelte centre samt være en stabil informationskanal til – og fra - medarbejderne. Netværket mødes om aktuelle dagsordener, videndeler og samarbejder om implementering af retningslinjer, god praksis for it-sikkerhed og formidling af GDPR til medarbejderne på tværs af organisationen. Det tegner rigtig godt, og jeg kan kun bakke op om, at dette arbejde prioriteres højt i centrene. GDPR-teamet er hårdt presset ressourcemæssigt, og der ligger en lang række større dokumentationsopgaver, som er blevet udskudt pga. tidsmangel. Disse større opgaver vil blive gennemgået senere i rapporten under den systematiske gennemgang af indsatsområder fra den forrige DPO-rapport. Ressourcerne bør være et strategisk fokus for 2022 for at det skal blive muligt at få indhentet de eksisterende hængepartier.

GDPR-området har stor opmærksomhed fra digitaliseringschefen i Ballerup Kommune. Det er positivt, da ledelsesopbakning er helt central for at sikre god dialog og forankring af opgaverne på tværs af organisationen.

GDPR er ofte en udskældt fagdisciplin, der beskyldes for at fjerne fokus fra kerneydelserne og synes at gøre livet besværligt for borgere og ikke mindst medarbejdere. For min del fokuserer jeg meget på, hvorfor GDPR opleves som svært og hæmmende i et fagområdet, og hvad der skal til for at hjælpe eller støtte op om at få det løst. Det kræver respekt mellem to eller flere fagligheder for at kunne lykkes og ikke mindst

kræver det ledelsesmæssig opbakning. Der er stor forskel på, hvor godt de enkelte centerchefer og ledere er klædt på til at håndtere GDPR. Der er behov for, at de forskellige ledelsesniveauer kontinuerligt bliver fagligt klædt på til at håndtere GDPR-implementeringen og prioritere GDPR-indsatsen i det enkelte center/afsnit. GDPR skal selvfølgelig ikke fylde hele dagsordenen, men vi skal anerkende, at forordningen eksisterer på lige fod med al anden lovgivning, som forvaltes i Kommunen. Ballerup Kommune arbejder målrette mod at borgerne har tillid til kommunen og GDPR-indsatsen skal understøtte, at vi passer godt på deres data.

5.3 Betydelige GDPR dagsordener

Implementeringen af GDPR i 2018 blev i mange kommuner anset som et projekt, der kom med en ekstra bevilling. Når alle detaljer var på plads, sluttede projektet. Ledelsen i mange kommuner overså, at behandling af persondata ændres løbende, og at der dermed skal etableres en proces og governance, der sikrer den løbende vedligeholdelse og implementering af GDPR i nye arbejdsprocesser, digitale systemer samt ved organisationsændringer. Ud over vedligeholdelse af dokumentationen for behandlingsaktiviteter støder betydelige internationale dagsordner til, der får de GDPR-ansvarlige til skulle løbe ekstra hurtigt for at leve op til GDPR.

5.3.1 SchremsII

Årets største tidsrøver har været spørgsmål, rådgivning og fortolkninger i forbindelse med Schrems II-dommen. Dommen er fra 2020 og giver kommunen som dataansvarlig store udfordringer med at anvende amerikanske cloud-løsninger. Persondata som gemmes i amerikanske cloud-løsninger betragtes som overførsel af persondata til et usikkert 3. land. Det skyldes, at USA's lovgivning ikke garanterer de sammen essentielle privatlivsrettigheder for borgerne i EU – eksempelvis har borgere ikke de samme klagemuligheder, og der er ikke de samme krav om gennemsigtige databehandlinger. Amerikansk lov giver efterretningstjenesterne frihed til at anmode tech-giganterne som Microsoft og Google om at udlevere data – også selvom databehandlingen sker i EU.

Helt kort: kommunen lever ikke op til GDPR, hvis data lagres i amerikanske cloud-løsninger. Der kan implementeret tekniske-, organisatoriske- og juridiske foranstaltninger, som nedbringer risikoen, men den elimineres aldrig helt.

Ballerup Kommune er meget opmærksom på disse udfordringer og GDPR-teamet arbejder intensivt på at sikre, at GDPR overholdes i indgåelsen af nye aftaler med databehandlere. Det giver ind i mellem anledning til frustration fra organisationen, når Schrems II kommer i vejen for brug eller indkøb af nye it-systemer, som skal understøtte arbejdet i centrene. Min anbefaling er, at ledere og medarbejdere klædes endnu bedre på til, at vurdere de GDPR-mæssige problemstillinger, så vi samme forståelse for de udfordringer vi møder.

Juridiske eksperter i Danmark spår, at det kræver ændring af den amerikanske lovgivning, før problemstillingen forsvinder helt, hvilket i givet fald vil tage lang tid. Indtil da er min principielle anbefaling, at Kommunen ikke overfører personoplysninger til amerikanske cloud-løsninger. I de sjældne tilfælde, hvor der er et uomtvisteligt behov for alligevel at benytte de problematiske cloud-løsninger, bør Kommunen sikre, at beslutningen tager udgangspunkt i en risikobaseret vurdering (risikovurdering og evt. en konsekvensanalyse - DPIA) som dokumenterer de tekniske- og organisatoriske foranstaltninger, der er implementeret for at nedbringe risikoen.

5.3.2 Google Workspace for Education

Sagen om Google Workspace for Education / GWfE (eller Google G Suite, som det hed tidligere) har fyldt meget i den offentlige debat. Datatilsynet har gennem 2½ år behandlet en anmeldelse om brud på persondatasikkerhed fra en borger i Helsingør kommune, om Helsingør Kommunes brug af GWfE i undervisningen på kommunens skoler. I efteråret udtalte Datatilsynet alvorlig kritik af Helsingør Kommune for ikke at have vurderet risikoen for de registrerede/skoleelevernes rettigheder ifm. med anvendelse af løsningen. Datatilsynet har af egen drift indledt en undersøgelse af, hvordan de andre 48 kommuner anvender GWfE, her iblandt Ballerup Kommune.

Efter min bedste overbevisning har Ballerup kommune godt styr på brugen af GWfE. Ballerup Kommune har tilbage i 2019 udarbejdet en DPIA (konsekvensanalyse) for brugen af GWfE, som løbende er blevet justeret. Administrationen på skoleområdet har arbejdet grundigt og seriøst med problemstillingerne og har et fuldstændigt overblik over indstillinger og brugeradgange. Der er udarbejdet retningslinjer og informationsmateriale til lærerne. Om dette er tilstrækkeligt, må Datatilsynet endeligt vurdere. Vi forventer en afgørelse af Ballerups sag i 2022.

Skoleområdet arbejdet sammen med DPO'en på at kortlægge hvilke persondata der sendes mellem området forskellige systermer, med fokus oprettelse og nedlæggelse af brugeradgange og rettigheder.

6. Sikkerhedsbrud

Sikkerhedsbrud er et evigt aktuelt tema i GDPR, som fylder en del i hverdagen. Ballerup Kommune har en meget veletableret beredskabsplan og beskrevet proces for håndtering af sikkerhedsbrud, via en online formular på kommunens INTRA, som derefter håndteres af GDPR-teamet med henblik på en vurdering af, hvorvidt hændelsen til indmeldes til Datatilsynet Medarbejdere i kommunen ved generelt hvordan og hvornår de skal anmelde et sikkerhedsbrud til GDPR-teamet.

Der blev i 2021 indmeldt 64 sikkerhedshændelser, hvoraf der var tale om 49 egentlige sikkerhedsbrud. Det er i sig selv ikke så interessant, udelukkende at se på om antallet falder eller stiger. Der skal løbende være fokus på sikkerhedsbrud, og hvorfor det er vigtigt at efterleve reglerne i GDPR. Der ved kan eventuelle mørketal mindskes.

Uopmærksomhed eller menneskelige fejl udgør langt den største andel af sikkerhedsbrud i Ballerup kommune – tilsvarende gør sig gældende på landsplan. Der er i Ballerup en god kultur omkring at indberette sikkerhedsbrud til GDPR-teamet, og det er meget værdifuldt. Det er forventeligt, at der vil ske menneskelige fejl i en travl hverdag. Det vigtigste er hvordan organisationen arbejder med at lære af sine fejl og adressere eventuelle problemstillinger i brugen af systemer og arbejdsgange. Det er et område jeg sammen med GDPR-teamet vil arbejde med i 2022.

7. Borgerhenvendelser

Der har været 5 borgerhenvendelser i 2021. De fleste henvendelser er sker på grund af dårlig eller misforstået kommunikation mellem borger og forvaltning.

Der har også være enkelte henvendelser, hvor borger er utilfreds med en afgørelse eller samarbejdet med Kommunen. Disse sager har sjældent noget med selve behandlingen af personoplysninger at gøre. Denne type henvendelser sendes videre til rette instans eller til borgerrådgiveren.

Der kommer en del mail i DPO mailboksen, som er gået decideret forkert, typisk fordi en borger eller ansat ikke kan finde andre kontaktmuligheder med kommunen eller administrationen. DPO mailen fremgår altid af den bekræftelse mail borgeren modtager for sin henvendelse fra kommunen. Det anbefales derfor, at centrene er opmærksomme på, hvordan borgere eller ansatte kommer i kontakt med rette instans, hvis de har spørgsmål til deres sag.

8. Opfølgning på anbefalinger fra seneste DPO-rapport (2020)

Den forrige DPO-rapport indeholdt en række anbefalinger og fokusområder for arbejdet med GDPR i Ballerup Kommune. Herunder gennemgår jeg en kort status for, hvordan det går med hvert af temaerne.

Læsevejledning:

Grøn: Anbefalinger og bemærkninger håndteret tilfredsstilende

Gul: Anbefalinger og bemærkninger er taget til efterretning, men Ballerup Kommune er ikke i mål med udførelsen af arbejdet

Rød: Anbefalinger som bør prioriteres, da de er kritiske ift. overholdelse af Databeskyttelsesforordningen.

Opfølgning fra 2020

Observation 1	Opfølgning og anbefaling	
Oplysningspligt (forud for indsamling og videregivelse af personoplysninger)	Ballerup har overordnet styr på oplysningspligten, både når oplysninger indsamles via digitale formularer, lægges i fagsystemer mm. Oplysningspligten er et løbende omdrejningspunkt, genbesøges og opdateret jævnligt. **Anbefaling:** Det anbefales, at der udarbejdes en oversigt over alle steder hvor oplysningspligten skal løftes og at arbejdet med oplysningspligten bliver genstand for et årligt review.	

Observation 2	Opfølgning og anbefaling	
Datasikkerhed (Brugeradgange logning)	Det er min vurdering at der overordnet er styr på oprettelse og nedlæggelse af brugere i kommunens IT-systemer. Der er ikke overblik over eller fast struktur for logning af medarbejderes it-adgange ved brug af kommunens systemer. Jeg er vidende om, at der gennemføres tilsyn og logning af en række af kommunens it-systemer. **Anbefaling**: Det anbefales at der indføres en struktureret og dokumenteret proces for logning af it-brugere i alle fagsystemer der indeholder persondata.	

Observation 3	Opfølgning og anbefaling	
Styring og ansvarsfordeling af GDPR-arbejdet	GDPR-teamet er forankret i Afsnit for Digitalisering og Forretningsudvikling. Et GDPR ambassadørnetværk er under opbygning, så GDPR forankres bedre i centrene. GDPR-teamet er en del af det fagligt fællesskab med de andre kommuners GDPR teams. Samarbejdet med DPO'en er rigtig godt. **Anbefaling:** For at understøtte kerneopgaverne i centrene, kan GDPR med fordel tænkes mere ind i arbejdet, så sikkerhed, regler og indsatser bliver mere synlige. Direktion, chefgruppen og andre ledere skal klædes på til at tænke GDPR ind i kerneopgaven. GDPR teamet har med sin nuværende bemanding ikke ressourcer til at håndtere den store mængde opgaver området dækker over. Det gælder for alle 4 kommuner. Et samarbejde kommunerne imellem, om de opgaver der er ens for alle, vil kunne afhjælpe nogle af de pukler af opgaver der ligger.	

Observation 4	Opfølgning og anbefaling	
DPO	Ballerup har robuste processer der sikre tilstrækkelig og rettidig inddragelse af DPO i alle spørgsmål vedrørende beskyttelse af personoplysninger. **Anbefaling:** Fortsættelse af det gode og konstruktive samarbejde.	

Observation 5	Opfølgning og anbefaling	
Fortegnelser (over behandlingsaktiviteter)	Der er udarbejdet fortegnelser for hvert center i kommunen, men de er ikke blevet opdateret siden 2018. Det er et krav i Databeskyttelsesforordningen, at fortegnelser genbesøges årligt. **Anbefaling:** Jeg er orienteret om at Fortegnelser er et fokusområde for 2022, og jeg anbefaler at det prioriteres. Fortegnelserne skaber et godt overblik over centrenes behandlingsaktiviteter og understøtter arbejdet med databeskyttelse lokalt. Det anbefales, at opdatering af Fortegnelserne bliver en del af et årligt review.	

Observation 6	Opfølgning og anbefaling	
Lovhjemmel (Punktet er meget bredt beskrevet, og der følges op på udvalgte temaer inden for lovhjemmel)	Min oplevelse er, at der er stor opmærksomhed i GDPR teamet, om der er korrekt lovhjemmel til en behandlingsaktivitet. I forbindelse med det forestående arbejde med at opdatere Fortegnelserne genbesøges lovhjemmelsspørgsmålet som en del af øvelsen. Arbejdet med oplysningspligten (se ovenfor) har betydet opdatering og sikring af korrekt lovhjemmel når der indsamles persondata om borgere, virksomheder og ansatte.	

	Deling af personoplysninger på tværs af forvaltningen er en svær øvelse, som Ballerup arbejder intenst med. Der er udarbejdet et juridisk notat, som forsøger at kortlægge rammerne for videregivelse af personoplysninger inden for forvaltningen. Det bliver spændende at følge den videre udvikling, og hvordan et så kompliceret område kan formidles til medarbejderne. SAPA projektet har inddraget GDPR teamet og DPO i arbejdet med at formulere en brugerstrategi som lever op til GDPR og samtidig er mulig at håndtere organisatorisk. **Anbefaling:** at der arbejdes videre med et koncept for hvad der må dele af personoplysninger på tværs af forvaltningen, for at sikre udveksling eller videregivelse af personoplysninger sker på det rigtige behandlingsgrundlag.	

Observation 7	**Opfølgning og anbefaling**	
Kryptering, anonymisering /pseudonymisering (Punktet er meget bredt beskrevet, og der følges op på udvalgte temaer)	Der er stort fokus på at der kommunikeres sikkert med borgere. Hvert center har retningslinjer for hvordan der sendes sikkert. Der er generelt udarbejdet retningslinjer for hvordan persondata håndteres ifm. høringssvar. **Anbefaling:** Det anbefales, at temaet om sikker kommunikation bliver en del af den generelle awarenes, da der her ofte sker (menneskelig) fejl. Ikke alle it-værktøjer understøtter en sikker kommunikation, så retningslinjer og procedurer er nødvendige – også at de overholdes i en travl hverdag. Det er et generelt opmærksomhedspunkt at arbejde med kryptering, anonymisering/pseudonymisering af data ifm. overførsel af data til fx forskningsinstitutioner og anvendelse af US cloudleverandører. Der er fortsat usikkerhed om anvendelse af US cloudleverandører, hvorfor det fortsat må anbefales ikke at indgå nye aftaler, hvor data gemmes i en US cloud. Udviklingen på dette område bør følges nøje.	

Observation 8	**Opfølgning og anbefaling**	
Informationssikkerhed og awarenes	Ballerup arbejder med at introducere et e-læringsværktøj om GDPR og Informationssikkerhed til alle medarbejdere. Samtid er der etableret et GDPR ambassadørnetværk som bliver talerør i GDPR henseender ud i organisationen. Det er hårdt arbejdet at implementere både et e-læringsværktøj og opbygge et netværk. **Anbefaling:** prioriter at få e-læringsværktøjet op og køre og fortsæt med at være tilstede i organisationen og formidl GDPR på en nærværende måde. Et højt vidensniveau blandt ansatte, er med til at mindste betjeningsfejl og sikkerhedsbrud mm.	

Observation 9	Opfølgning og anbefaling	
Databehandlere og databehandleraftaler	Der er styr på processerne omkring indgåelse af databehandleraftaler. Opgaven er stor og ressourcekrævende og hele anskaffelsesproceduren skal fungere for at ressourcerne udnyttes optimalt. Det er krav i forordningen at man som dataansvarlig skal føre tilsyn med sine databehandlere. Ballerup har en veldokumenteret proces for at føre tilsyn med sine databehandlere. Det er en meget krævende opgave som ikke altid har 1. prioritet. **Anbefaling:** Som følge af Schrems-II dommen skal kommunerne være særlig opmærksomme på overførsler af personoplysninger til 3. lande. Det anbefales at der udarbejdes en oversigt over alle databehandlere og om de overfører persondata til usikre 3. lande. Tilsyn med databehandlere: Det er et krav i GDPR. at der føres tilsyn med kommunens databehandlere. Det anbefales at der lægges en plan for tilsyn med databehandlere - ud fra hvilke persondata de behandler og hvor mange. Der er et efterslæb i forhold til at føre tilsyn med alle nødvendige databehandlere, det bør prioriteres. Også her er potentiale i at arbejde sammen med de andre 3 kommuner, da det er præcis de samme IT revisionsrapporter kommunerne modtager og som danner udgangspunkt for tilsynet. Det anbefales at se på. om der er potentiale i at samarbejde med de andre 3 kommuner om indgåelse af databehandleraftaler. Det vil kunne aflaste arbejdsbyrden i GDPR teamet.	

Observation 10	Opfølgning og anbefaling	
Risikovurderinger og konsekvensanalyser (DPIA) (for behandlingsaktiviteter og IT systemer)	Der er udarbejdet en solid og brugervenlig skabelon for risikovurderinger. Der mangler en prioriteret og dokumenteret tilgang til at arbejde med risiko. GDPR teamet er klædt på til arbejdet med risikovurdering, men inddrages ofte for sent ift. til at kunne udarbejde en risikovurdering eller konsekvensanalyse rettidigt. Konsekvensanalyser er omfangsrige og skal udarbejdes når risikoen er stor for de registrerede. DPO'en inddrages i arbejdet, de gange der er udarbejdet en konsekvensanalyse. **Anbefaling**: Datatilsynet har i sine afgørelser praksis for at bede om dokumentation for vurderingen af risikoen for en given behandlingsaktivitet. Der ligger en stor opgave i retrospektivt at få udarbejdet risikovurderinger for alle be-	

	handlingsaktiviteter og IT systemer som behandler persondata. Det anbefales at denne opgave prioriteres i 2022 evt. i samarbede med de 3 andre kommuner. Det anbefales ligeledes at der skabes et overblik over om der mangler at blive udarbejdet konsekvensanalyser. Fokus på at GDPR temaet inddrages rettidigt i anskaffelsesprocessen.	

Observation 11	Opfølgning og anbefaling	
Databrud (Sikkerhedsbrud og sikkerhedshændelser)	Ballerup har en formular på Intra hvor sikkerhedsbrud kan anmeldes til GDPR temaet, som forestå den videre behandling. Det er en velfungerende proces der er alment kendt i organisationen. Jeg orienteres og inddrages rettidigt og tilstrækkeligt i de hændelser der opstår. Der er udarbejde procedurer (actioncard) for håndtering af sikkerhedsbrud. Alle sikkerhedsbrud og hændelser dokumenteres. **Anbefaling:** Arbejde mere i dybden med, hvordan organisationen lærer af sine sikkerhedsbrud. Det bliver et fokusområde for mine tilsyn med kommunen i 2022.	

Observation 12	Opfølgning og anbefaling	
De registreredes rettigheder • Ret til indsigt • Ret til berigtigelse • Ret til sletning • Ret til begrænsning af behandling • Ret til dataportabilitet • Automatisk behandling	Ballerup Kommune har fokus på registreredes rettigheder i alle spørgsmål vedrørende behandling af personoplysninger. De registreredes rettigheder oplyses bl.a. i oplysningspligten. Der er meget få indsigtsbegæringer og de er håndteret godt inden for rammerne af GDPR. **Anbefaling:** Sikre at der foreligger sikker dokumentation for overvejelser, risikovurdering og endelige beslutninger vedrørende de registreredes rettigheder. Overblik over retningslinjer og processer for imødekommelse af de registreredes rettigheder.	

9. Planlagte tilsyn 2021

Der blev gennemført 1 planlagt tilsyn i 2021. Der var tale om et "skrivebordstilsyn", hvor vi sammen gennemgik, hvordan et skriftligt tilsyn fra Datatilsynet skulle håndteres, og om den ønskede dokumentation var til stede.

Planlagt tilsyn 1	Observationer og anbefaling	
Administration af adgangs-rettigheder i socialforvaltningen - Adgangsbegrænsning og brugerstrategi på socialområdet 1. Liste over it-systemer der anvendes i socialforvaltningen som behandler oplysninger om fysiske personer. 2. Listen skal omfatte en beskrivelse af hvilke oplysninger, der behandles i systemerne 3. Hvordan styrer kommunen adgangsrettighederne til systemerne? 4. Kommunens generelle politikker for adgangskontrol, audit og stikprøver for uautoriseret adgangsforsøg.	GDPR teamet: Der foreligger en procedure for hvordan skriftlige tilsyn håndteres og hvem der skal inddrages. Det er afprøvet tilfredsstillende i det konkrete tilfælde. Der kan trækkes en liste fra Kitos over it-systemer, her i indgå også hvilke data der behandles i systemerne. Håndtering af adgangsrettigheder til systemerne er beskrevet og dokumenteret. Der foreligger ikke umiddelbart dokumentation for Ballerups håndtering af audit og stikprøver for uautoriseret adgangsforsøg på socialområdet. **Anbefaling:** Det anbefales at få formuleret en generel politik for logning og stikprøver for alle it-systemer i kommunen. Der foreligger dokumentation for tilsyn og logning ifm. med de systemer der indgår i den årlige IT-revisionen Datatilsynet anbefaler tilsyn på udvalgte bruger 3-4 gange om året, for systemer der behandler mange følsomme persondata om borgerne. Adgangskontrol og logning vil være en et af mine fokusområder i 2022.