April 2021

Administrationens kommentarer til GDPR-årsrapporten

1. indledning

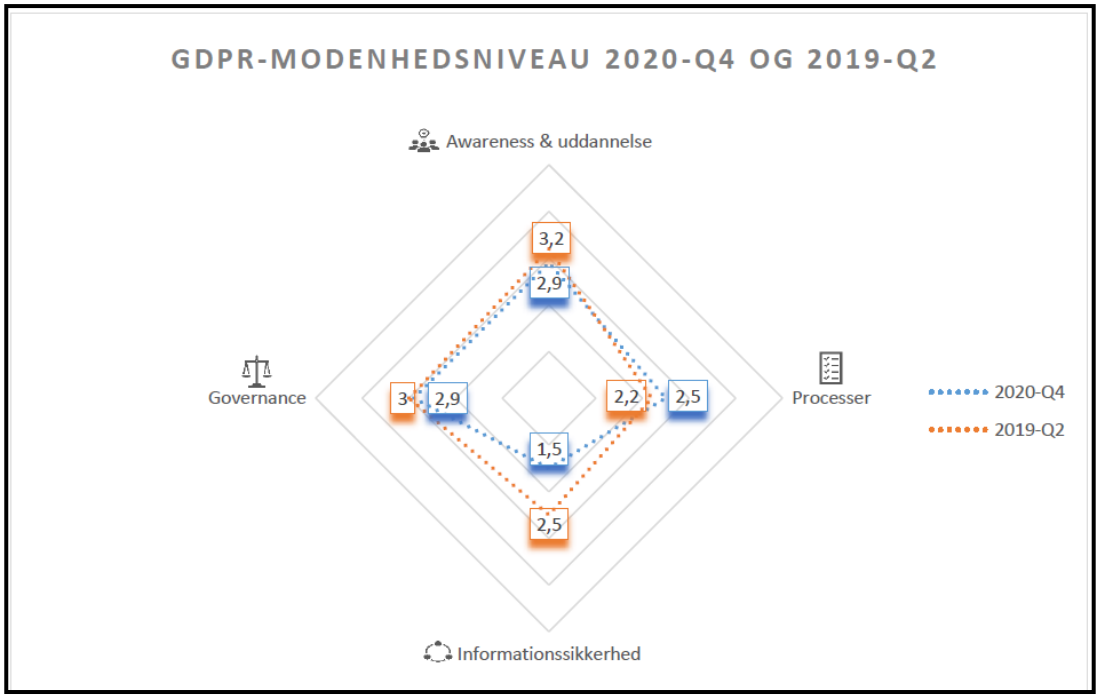
Administrationen har modtaget databeskyttelsesrådgiverens (DPO) årsrapport for 2020.

Rapporten adresserer 35 forskellige forhold i relation til GDPR, og den indeholder 10 anbefalinger til indsatsområder. I det følgende gives en status på GDPR-arbejdet i Ishøj Kommune.

Årsrapporten er i høj grad baseret på en modenhedsmåling, som DPO'en udførte i september 2020. Dette notat vil derfor først fokusere på resultaterne heri, samt udviklingen siden sidste årsrapport. Herefter gennemgås status på DPO'ens 10 anbefalinger og resultaterne i årsrapporten gennemgås overordnet. En fuld gennemgang af de 35 områder i årsrapporten findes i bilag 1.

2. Årsrapportens resultater og udviklingen heri siden sidste årsrapport

Hvis vi sammenligner med resultaterne fra 2019, er den samlede GDPR-modenhed i organisationen desværre gået en lille smule tilbage – samlet 0,1 point (se figur nedenfor).



Den manglende fremgang kan der være mange forklaringer på. For det første er der tale om en selvevaluering, så besvarelserne afhænger i høj grad af kendskabet til GDPR og 'selvopfattelsen' hos de pågældende respondenter (som er ledere i kommunen).

Herudover har håndteringen af Covid-19 fyldt meget i organisationen i 2020, hvilket også har haft betydning for arbejdet med GDPR. Således er størstedelen af de awarenessaktiviteter (f.eks. GDPR-cafeer, quizzer mv.), som var planlagt i 2020 blevet aflyst eller udsat på grund af COVID-19, og tilsvarende blev ansættelsen af en GDPR-konsulent udskudt fra marts til medio august 2020, og effekten af at have en dedikeret GDPR-ressource kan derfor ikke ses i modenhedsmålingen.

Implementeringen af det indkøbte e-læringsystem (Moch), som blev bevilliget af byrådet i foråret 2020, blev ligeledes forsinket på grund af Covid-19 og udfordringer med brugerstyringen. Medarbejderne nåede derfor ikke at gennemføre e-læringsmodulet inden modenhedsmålingen, hvilket også kan have haft en negativ ef-

fekt på modenhedsmålingens resultater. Nu er Moch implementeret, og i perioden medio januar til medio april 2021 har knapt 1.200 af kommunens ansatte gennemført og bestået e-læringsmodulet i GDPR.

Det største fald i modenheden ses dog inden for kategorien informationssikkerhed, og her skyldes den væsentlig lavere selvvurdering, at vi er blevet klogere på hvilke krav der stilles til f.eks. risikovurderinger efter GDPR og til at arbejde efter ISO27001. Resultatet for 2019 har således på dette område ikke vist et retvisende billede af organisationens modenhed.

Modenhedsmålingen fra 2019 og 2020 er heller ikke fuldt ud sammenlignelige, da der er kommet flere respondenter med i 2020 (64 i 2020 mod 49 i 2019), og der er målt på færre modenhedskriterier end i 2019 (35 i 2020 mod 40 i 2019).

Det er dog positivt, at der ses en betydelig fremgang på de områder, som administrationen har arbejdet mest målrettet med i 2020, nemlig kategorien processer (procedurer), men det samlede resultat levner plads til forbedring.

For en mindre kommune som Ishøj, er det dog en udfordring med de mange krav i GDPR, især kravene omkring dokumentation og risikovurdering, der kræver mange ressourcer.

3. Status samt forslag til handleplan på de 10 indsatsområder, som DPO'en anbefaler i sin årsrapport

På baggrund af modenhedsmålingen og de nøgletal, som administrationen har indberettet til DPO'en, er denne kommet med anbefalinger til 10 indsatsområder, som Ishøj Kommune bør prioritere i arbejdet med GDPR, for at opnå en bedre compliance på GDPR-området.

Administrationen redegør nedenfor for status på de 10 områder, og kommer med et forsalg til handleplan i forhold til disse. Koncernledelsen har herudover d. 21. april 2021 besluttet at nedsætte en arbejdsgruppe bestående af 4 centerchefer, som skal prioritere og tydeliggøre ansvarsfordelingen i forhold til de anbefalede indsatser.

De ti anbefalede indsatsområder

Anbefaling fra DPO	**Forslag til kontrol fra DPO**	**Status fra administrationen**	**Forslag til handleplan fra administrationen**
Årshjul for GDPR-arbejdsopgaver	Etablere et årshjul for GDPR-arbejdsopgaver som fundament til gennemførelse af løbende GDPR-opgaver centralt og decentralt i kommunen.	Dette er ikke udarbejdet fra central hånd, men enkelte centre/områder har udarbejdet årshjul for deres egne GDPR-opgaver.	Der vil blive udarbejdet et årshjul for GDPR-opgaver i løbet af 2. halvår af 2021 af sikkerhedsgruppen.
Inddragelse af DPO'en ved indkøb af nye IT-systemer	Etablere procedure eller koncept, der sikrer, at kommunen inddrager DPO'en tilstrækkeligt i forbindelse med anskaffelse af nye it-løsninger til brug for behandling af persondata.	Det fremgår bl.a. af kommunens *håndbog for informationssikkerhed*, at DPO'en skal inddrages når der tages ny teknologi i brug, der indkøbes nye systemer eller, hvis man opstarter en ny behandlingsaktivitet, f.eks. et projekt. Det fremgår dog af nøgletallene for 2020, at DPO'en kun er blevet inddraget i 1 ud af 6 indkøb af nye systemer. Dette tyder på, at der ikke er tilstrækkelig ledel-	Det skal tydeliggøres i relevante procedurer og retningslinjer, hvornår DPO'en skal inddrages bl.a. via link til håndbog for informationssikkerhed på Uglen. Herudover vil kravet om inddragelse af DPO'en blive kommunikeret til organisationen via et nyhedsbrev. De systemansvarlige (typisk centercheferne) skal

Anbefaling fra DPO	Forslag til kontrol fra DPO	Status fra administrationen	Forslag til handleplan fra administrationen
		sesmæssig opmærksomhed på denne forpligtelse.	sikre ledelsesmæssig opmærksomhed, så DPO'en inddrages i forbindelse med indkøb af nye IT-systemer.
Etablere et register for databehandlere	Etablere et centralt register for databehandlere, som afspejler status for databehandleraftale, risici, tilsynsstatus og eventuelle kritiske mangler samt bruge registreret som et prioriterings- og styrings-værktøj til kommunens tilsyn med *egne* databehandlere baseret på risici forbundet med persondatabehandling.	Hovedparten af databehandleraftalerne er registeret i sbsys. Digitalisering og IT har en oversigt (excel-ark) over databehandleraftalerne. Vi har dog ikke det fulde overblik over alle indgåede databehandleraftaler, og der fremgår ikke alle de nævnte oplysninger af den pågældende oversigt.	Digitalisering og IT stiller et system til rådighed (f.eks. Kitos eller Secure-aware), der understøtter organisationen i at dokumentere kommunens it-portefølje. Målet er, at dette er på plads inden udgangen af 2021. Der udarbejdes en intern governance-model med rolletildelinger såsom "systemejer" og "systemansvarlig". De systemansvarlige er ansvarlige for, at nye systemer/ændringer heri indrapporteres til databehandlerregisteret. Digitalisering og IT er ansvarlige for at systemet er ajourført i overensstemmelse med den vedtagne governance-model.
Procedure for tilsyn med databehandlere	Etablere en nedskrevet procedure, som sikrer, at kommunen kan føre tilsyn med databehandleres opfyldelse af databehandleraftalers betingelser, herunder implementering og opretholdelse af sikkerhedsforanstaltninger for beskyttelse af kommunens persondata. Proceduren skal tage højde for, at kommunen dels skal føre tilsyn med egne databehandlere, og dels skal gennemgå tilsynsrapporter fra tilsynsfunktionen i DSD samt udarbejde tilsynserklæringer om	Der ligger en procedure for tilsyn med databehandlere i udkastform. Denne er dog ikke færdiggjort og godkendt af Koncernledelsen (KCL) endnu.	Proceduren færdiggøres af sikkerhedsgruppen og forelægges for KCL i 2. halvår af 2021.

Anbefaling fra DPO	Forslag til kontrol fra DPO	Status fra administrationen	Forslag til handleplan fra administrationen
	tilsynsrapporter fra tilsynsfunktionen.		
Gennemføre tilsyn med databehandlere	Gennemføre flere tilsyn med *egne* databehandlere på baggrund af en plan for tilsyn, herunder faktisk gennemgå tilsynsrapporter fra tilsynsfunktionen i Den Storkøbenhavnske Digitaliseringsforening (DSD) samt udarbejde tilsynserklæringer om tilsynsrapporter fra tilsynsfunktionen.	Der er kommet gang i det fælles tilsyn, men de systemansvarlige udfører pt. stort set ikke tilsyn på de systemer, som ikke er en del af det fælles tilsyn i DSD.	Når proceduren for tilsyn med databehandlere er godkendt af KCL, udvælger sikkerhedsgruppen hvilke systemer, der skal føres tilsyn med. Det er målet, at der inden udgangen af 2021 føres tilsyn med min. 5 databehandlere (som ikke er omfattet af det fælles tilsyn i DSD-regi) og at tilsynsrapporterne fra DSD-tilsynene gennemgås.
Etablere en proces for risikovurderinger	Etablere en proces, der sikrer, at kommunen løbende gennemfører dokumenterede risikovurderinger efter GDPR med fokus på persondatabeskyttelse for de borgere (og andre personer), som kommunen behandler persondata om. Dette er navnlig relevant, før kommunen behandler persondata i nye it-løsninger.	Der ligger en procedure for risikovurdering i udkastform. Denne er dog ikke færdiggjort og godkendt af Koncernledelsen endnu. Det er dog en udfordring, at arbejdet med risikovurderinger kræver mange ressourcer. Risikovurderinger vurderes til at være den GDPR-opgave, der kræver flest ressourcer, da det er en øvelse, der skal foretages kontinuerligt. De begrænsede ressourcer gør, at det er de personer, der trækkes på i forvejen, som kan udfærdige risikovurderinger. Derfor er det svært for fagområderne at leve op til dette ansvar.	Proceduren færdiggøres af sikkerhedsgruppen og forelægges for KCL i 2. halvår af 2021. Det er administrationens vurdering, at der vil være behov for ekstern bistand for at indhente efterslæbet på opgaven med at foretage risikovurderinger. Herudover kræver det uddannelse af medarbejdere i Digitalisering og IT og på fagområderne for at løfte opgaven med risikovurderinger fremadrettet.
Implementering af passende sikkerhedsforanstaltninger	Etablere en proces, der sikrer, at kommunen på baggrund af risikovurderinger efter GDPR implementerer passende sikkerhedsforanstaltninger for beskyttelse af persondata, hvis risiko for	Der arbejdes i dag ikke systematisk med processen om sikkerhedsforanstaltninger ift. vurderede risici. Der foretages ad hoc sikkerhedsforanstaltninger i de enkelte fagcentre, men dette arbejde følger for-	Digitalisering og IT udarbejder en risikohåndteringsplan, som skal godkendes i KCL inden udgangen af 2021. Arbejdet udføres efter ISO27001, og der inddra-

Anbefaling fra DPO	Forslag til kontrol fra DPO	Status fra administrationen	Forslag til handleplan fra administrationen
	persondata er for høj (risikohåndtering).	mentlig ikke en godkendt standard (f.eks. ISO27001).	ges ekstern konsulenthjælp til arbejdet.
Sikkerhedstest	Etablere en proces for sikkerhedstest af systemer, der understøtter behandlingsaktiviteter (behandling af persondata) i kommunen, der sikrer løbende afprøvning og vurdering af implementerede tekniske sikkerhedsforanstaltningers effektivitet.	Der arbejdes i dag ikke systematisk med processen om sikkerhedstests. Den nuværende beredskabsplan er ikke ajourført, og det er i denne sikkerhedstest bør fremgå. Kommunens nuværende ISMS (information security management system) fra Neupart er ikke ajourført.	Der etableres overblik over processer og snitflader på tværs af systemer. På baggrund i risikovurdering og antal afhængigheder laves plan for hvilke sikkerhedstest der skal laves selvstændigt (af Ishøj). Arbejdet laves i sammenhæng med beredskabsplan, da en del delopgaver er overlappende. Arbejdet bør dokumenteres i et ISMS.
Tærskelvurderinger	Etablere en nedskrevet procedure for tærskelvurdering, der sikrer, at kommunen kan identificere, om planlagte nye behandlinger af persondata i kommunen er underlagt krav om gennemførelse af en konsekvensanalyse forud for behandling af persondata.	Der ligger en procedure for risikovurdering i udkastform, hvori det også beskrives, hvornår der skal foretages konsekvensanalyse. Denne procedure er dog ikke færdiggjort og godkendt af Koncernledelsen endnu.	Proceduren færdiggøres af sikkerhedsgruppen og forelægges for KCL i 2. halvår af 2021
Intern kontrol med overholdelse af politikker for databeskyttelse og GDPR i kommunen	Gennemføre løbende stikprøvekontroller med overholdelse af politikker og GDPR i kommunen på baggrund af et koncept og en årlig plan for kontrol, som tager højde for risici for persondata i kommunen (risikobaseret tilgang).	Dette er ikke systematiseret fra central hånd, men gøres ad hoc mange steder.	Sikkerhedsgruppen udarbejder en procedure/tjekliste for intern kontrol inden udgangen af 2021 i samarbejde med fagcentrene. Der tages afsæt i principperne for ISO27001 og kontrolopgaverne samt ansvaret herfor indarbejdes i det kommende årshjul for GDPR-opgaver.

4. Prioritering af GDPR-indsatsen og resultaterne i årsrapporten

Udover de 4 indsatsområder, som DPO'en har anbefalet vil følgende opgaver blive prioriteret i 2021 i det omfang, der er ressourcer til det:

1. **Opdatering af håndbogen *Regler for informationssikkerhed* (skulle have været opdateret i 2020)**
2. **Udarbejde procedure, som sikrer mindst én årlig kommunikation af databeskyttelsespolitikker**
3. **Udarbejde procedure for dataminimering, formålsbegrænsning og datakvalitet**

4. Udarbejde beredskabsplan