Bilag 1: Status på de 35 områder fra årsrapporten

Som nævnt i indledningen adresserer DPO'ens årsrapport 35 forskellige forhold i relation til GDPR.

Årsrapporten er i høj grad baseret på en modenhedsmåling, som DPO'en udførte i september 2020 samt nøgletal fra administrationen.

Nedenfor er en fuld gennemgang af de 35 områder og en status på udviklingen siden 2019.

Governance

Nr.	Titel i rapport	Beskrivelse	Status
1	Direktion og ledelse understøtter GDPR-compliance	For at nå i mål med GDPR er det nødvendigt, at ledelsen understøtter arbejdet og har efterlevelse af GDPR som en høj prioritet	Her ses en fremgang siden målingen i 2019, og niveauet er acceptabelt.
2	Roller og ansvar	For at nå i mål med GDPR er det nødvendigt, at der er en tydelig og nedskrevet organisering, som klart definerer roller og ansvar.	Her ses en fremgang siden målingen i 2019, og niveauet er acceptabelt. Efter modenhedsmålingen i 2019, blev organiseringen ændret. Med den nye organisering er der nedsat en central sikkerhedsgruppe samt et GDPR-koordinatorforum, hvor alle centre er repræsenteret med min. 1 medarbejder. Med den nye organisering er fordeling af ansvar og arbejdsopgaver konkretiseret og samtidig er der lagt vægt på, at de lokale sikkerhedskoordinatorer opkvalificeres.
3	Databeskyttelsespolitikker	Det er et krav i GDPR, at kommunen har nedskrevne og godkendte databeskyttelsespolitikker. Politikkerne skal bruges som dokumentation for, at kommunen udstikker retningslinjer til de ansatte i forhold til behandling af personoplysninger.	Her ses en fremgang siden målingen i 2019, og niveauet er acceptabelt.
4	Opdatering af databeskyttelsespolitikker	Der skal desuden være en klar procedure og ansvarsfordeling, som sikrer,	Vi er gået tilbage på dette punkt i målingen siden 2019, men niveauet er stadig acceptabelt.

Nr.	Titel i rapport	Beskrivelse	Status
		at politikkerne holdes opdaterede.	*Strategi for Informationssikkerhed* skal opdateres hvert 4. år i forbindelse med valg af nyt Byråd. Håndbogen *Regler for Informationssikkerhed* skal opdateres årligt og godkendes af Koncernledelsen. Håndbogen blev *ikke* opdateret i 2020 som planlagt.
5	Kommunikation af databeskyttelsespolitikker	Kommunen skal kunne dokumentere, at databeskyttelsespolitikkerne er kommunikeret ud i organisationen samt til nye medarbejdere, så de ansatte ved, hvilke regler de skal efterleve.	Vi er gået tilbage på dette punkt i målingen siden 2019, og niveauet bør hæves. Kommunens databeskyttelsespolitikker er tilgængelige på kommunens intranet (uglen) og bliver kommunikeret i forbindelse med vedtagelse og revidering. Kommunen har dog ikke en procedure, som sikrer mindst én årlig kommunikation til ledere og medarbejdere, hvilket gør, at kommunen scorer lavt i målingen i år.
6	Monitorering af overholdelse af databeskyttelsespolitikker og GDPR-compliance	I forhold til GDPR er det ikke tilstrækkeligt at have en politik. Der er også krav om, at kommunen følger op på, om medarbejderne efterlever reglerne i praksis.	Vi er gået tilbage på dette punkt siden 2019, og niveauet bør hæves Dette er ikke systematiseret fra central hånd, men gøres ad hoc mange steder. DPO'en har fremhævet dette i sine anbefalinger, hvorfor det bør prioriteres i 2021.
7	Årshjul for GDPR-arbejdsopgaver	Et årshjul er en god måde at dokumentere, at man efterlever de krav der er til kontroller, opdatering af procedurer, politikker, tilsyn mv. i GDPR.	Status på dette punkt er uændret siden sidste år, og niveauet bør hæves. Dette er ikke udarbejdet eller implementeret fra central hånd. DPO'en har fremhævet dette i sine anbefalinger, hvorfor udarbejdelsen af et årshjul vil blive prioriteret i første halvår af 2021.

Awareness og uddannelse

Nr.	Titel i rapport	Beskrivelse	Status
8	Awareness	Det er et krav i GDPR, at man sikrer sig, at ens medarbejdere er bekendte med og mindes om reglerne i GDPR.	Vi er gået tilbage i modenhedsmålingen siden 2019, men niveauet er acceptabelt. Flere af de planlagte awareness aktiviteter (GDPR-cafeer, quiz mv.) er ikke blevet gennemført i 2020 pga. coronarestriktioner.
9	Uddannelse/træning	Ud over awareness er der også krav om, at kommunen gennemfører målrettede uddannelsesaktiviteter i form af kurser eller e-læring.	Modenhedsmålingen viser en lille samlet fremgang på dette punkt, men viser også at der væsentlig forskel mellem de forskellige fagområder. Niveauet bør dog stadig hæves. Der er indkøbt et e-læringsværktøj (moch), som både indeholder et GDPR- og et cybersikkerhedskursus. GDPR-kurset er igangsat i organisationen i januar 2021, og det er planen at de ansatte skal recertificeres én gang årligt. De lokale sikkerhedskoordinatorer i kommunens ni centre samt andre medarbejdere, som beskæftiger sig med GDPR, har herudover i august 2020 været på en heldagskursus i GDPR.

Processer

Nr.	Titel i rapport	Beskrivelse	Status
10	Fortegnelse	I GDPR er der et krav om, at kommunen har en fortegnelse over sine behandlingsaktiviteter. En fortegnelse er en slags beskrivelse af alle kommunens behandlingsaktiviteter med persondata, hvori der bl.a. står, hvad formålet er med behandlingen, hvilken lovhjemmel kommunen har samt, hvilke typer af	Der ses en fremgang i målingen siden 2019, og niveauet er acceptabelt. I august 2020 reviderede datatilsynet dog deres krav til fortegnelser, så fortegnelserne for 2021 skal tilpasses til de nye krav.

Nr.	Titel i rapport	Beskrivelse	Status
		personoplysninger, der behandles.	
11	Indsamling til sagligt formål (data-minimering)	I GDPR er der et krav om dataminimering, hvilket vil sige, at der kun må indhentes og gemmes de oplysninger, som er nødvendige for at opnå ens formål.	Der ses en lille fremgang i målingen siden 2019, men niveauet ligger stadig lidt lavt. Princippet om dataminimering overholdes generelt, men der mangler en nedskrevet procedure. Denne udarbejdes hurtigst muligt.
12	Datakvalitet	I GDPR er der krav om rigtigheden, af de data kommunen gemmer om borgerne. Det vil sige, at oplysningerne skal være opdaterede samt, at forkerte oplysninger enten skal berigtiges eller slettes.	Der ses en fremgang i målingen siden 2019, men niveauet ligger stadig lidt lavt. Princippet om datakvalitet efterleves, men der mangler en nedskrevet procedure. Denne udarbejdes hurtigst muligt.
13	Formålsbegræsning	I GDPR er der krav om, at personoplysninger ikke må bruges til andre formål, end dem de er indsamlet til.	Der ses en fremgang i målingen siden 2019, men niveauet ligger stadig lidt lavt. Princippet om formålsbegræsning efterleves, men der mangler en nedskrevet procedure. Denne udarbejdes hurtigst muligt.
14	Opbevaringsbegrænsning	I GDPR er der krav om, at personoplysninger ikke må gemmes i længere tid, end hvad der er nødvendigt af hensyn til sagsbehandlingen.	Der ses en fremgang i målingen siden 2019, men niveauet ligger stadig lidt lavt. Koncernledelsen har i august 2020 vedtaget en procedure for opbevaringsbegrænsning. Proceduren kræver dog også en lokal/decentral indsats.
15	Gyldigt samtykke efter GDPR	I GDPR er der meget specifikke krav til et samtykke. Et samtykke skal være: - Frivilligt	Der ses en fremgang i målingen siden 2019, og niveauet et acceptabelt.

Nr.	Titel i rapport	Beskrivelse	Status
		- Specifikt - Utvetydigt - Informeret	Samtykke har været et fokusområde i både oplæg og caféer. Der er desuden udarbejdet en skabelon, som kommunens ansatte kan bruge til at indhente samtykke efter reglerne i GDPR.
16	Oplysningspligt	I GDPR er der et krav om oplysningspligt. Det vil sige, at når kommunen behandler og indsamler personoplysninger om en person, har vi pligt til at informere denne om behandlingen.	Der ses en fremgang i målingen siden 2019, men niveauet ligger stadig lidt lavt. Koncernledelsen har i august 2020 vedtaget en procedure for håndtering af de registreredes rettigheder, som også omfatter oplysningspligten. Oplysningspligten har været et fokusområde i både oplæg og caféer. Der er desuden udarbejdet skabeloner, som kan bruges til at opfylde oplysningspligten efter GDPR.
17	Håndtering af registreredes (borgernes) rettigheder	I GDPR har de registrerede (dvs. dem vi behandler oplysninger om) en række rettigheder, herunder retten til: - Indsigt i de oplysninger, vi behandler om dem - Få berigtiget forkerte oplysninger - Få oplysninger slettet - Gøre indsigelse mod behandling af deres oplysninger mv. Disse rettigheder skal kommunen kunne håndtere.	Der ses en fremgang i målingen siden 2019, men niveauet ligger stadig lidt lavt. Der er udarbejdet en procedure for håndtering af de registreredes rettigheder, som er godkendt af koncernledelsen i august 2020.
18	Persondatasikkerhedsbrud	I GDPR er der krav om, at sikkerhedsbrud med persondata indberettes til Datatilsynet inden for 72 timer, hvis der er en risiko for den registreredes mulighed for at udøve sine	Der ses en fremgang i målingen siden 2019, og niveauet er acceptabelt. Kommunen har en velbeskrevet og velfungerende procedure

Nr.	Titel i rapport	Beskrivelse	Status
		rettigheder. Hvis der er en høj risiko for den registrerede, skal han eller hun også orienteres om bruddet uden unødig forsinkelse.	for håndtering af sikkerhedsbrud. Proceduren er i 2020 blevet opdateret således at de lokale sikkerhedskoordinatorer selv skal anmelde centrets sikkerhedsbrud.
19	Register for databehandlere	Der skal indgås databehandleraftaler med de virksomheder, som behandler persondata på Kommunens vegne (eks. dem som leverer vores IT-systemer). Databehandleraftalerne skal gemmes i et register (eks. SBSYS), så kommunen har styr på dem.	Niveauet er uændret siden målingen i 2019, og ligger for lavt. DPO'en har fremhævet dette i sine anbefalinger, hvorfor udarbejdelsen af et register for databehandlere bør prioriteres i 2021 Administrationen har registreret omkring 200 databehandleraftaler i SBSYS, men der er formentlig indgået flere, som ikke er registreret.
20	Kvalitetssikring af databehandlere (due diligence)	Inden kommunen indgår en databehandleraftale med en leverandør, skal kommunen sikre sig, at leverandøren har en tilstrækkelig høj sikkerhed omkring behandling af personoplysninger.	Der er i 2020 udarbejdet et spørgeskema til formålet. Proceduren for indgåelse af databehandleraftaler skal redigeres, så due diligence (behørig omhu) tilføjes. Vi er dog gået frem på dette punkt i målingen, og niveauet er acceptabelt.
21	Kvalitetssikring af databehandleraftaler	En databehandleraftale skal stille en række specifikke krav til databehandlerne, herunder at de iværksætter passende organisatoriske og tekniske sikkerhedsforanstaltninger i forhold til de personoplysninger, de behandler.	Skabelonen er i 2020 opdateret i med udgangspunkt i en ny skabelon fra Datatilsynet. Vi er gået frem i målingen på dette punkt, og niveauet er acceptabelt.
22	Indgåelse af databehandleraftaler	Det er et krav i GDPR, at der indgås en databehandleraftale, når kommunen gør brug af en databehandler.	Administrationen har udarbejdet en procedure for indgåelse af databehandleraftaler.

Nr.	Titel i rapport	Beskrivelse	Status
			Det vurderes, at der er indgået databehandleraftaler med mindst 75 % af de databehandlere, som kommunen bruger, men vi skal op på 100 %, før vi lever op til kravene i GDPR
23	Procedure for tilsyn med databehandlere	Det er et krav i GDPR, at kommunen fører tilsyn med sine databehandlere for at sikre, at de beskytter kommunens personoplysninger tilstrækkeligt. Dette skal dokumenteres via en procedure.	Vi ligger meget lavt i målingen, da vi ikke har en godkendt procedure for tilsyn med databehandlere. Der er udarbejdet et udkast til procedure for tilsyn med databehandlere, som skal færdiggøres og godkendes af KCL. DPO'en har fremhævet dette i sine anbefalinger, hvorfor det bør prioriteres i 2021.
24	Tilsyn med databehandlere	Det er et krav i GDPR, at kommunen fører tilsyn med sine databehandlere for at sikre, at de beskytter kommunens personoplysninger tilstrækkeligt.	Vi ligger meget lavt i målingen, da Ishøj Kommune ikke selv har ført tilsyn med kommunens databehandlere og vi ikke har en tilsynsplan. Der er etableret et fælles tilsyn i regi af DSD, så der bliver ført tilsyn med nogle af de systemer, som flere af kommunerne i DSD bruger. Resultaterne af de fælles tilsyn skal dog stadig vurderes af de enkelte kommuner, hvilket vi er gået i gang med.
25	Risikovurderinger efter GDPR	Det er en grundsten i GDPR, at man skal have en risikobaseret tilgang til behandling af personoplysninger. Det vil sige, at der skal udarbejdes en risikovurdering, når kommunen eks. ændrer arbejdsgang eller tager ny	Dette er et meget ressourcekrævende arbejde. Administrationen har ikke ressourcer pt. til at gøre dette fuldt ud, så det gøres kun i begrænset omfang.

Nr.	Titel i rapport	Beskrivelse	Status
		teknologi i brug i behandlingen af personoplysninger for at sikre, at det ikke medfører en unødig høj risiko for de registrerede.	På dette punkt ses en nedgang i niveau i forhold til sidste års måling. Dette skyldes, at vi er blevet klar over, hvilke krav der stilles til risikovurderinger efter GDPR. Der er udarbejdet udkast til procedure for risikovurdering, som skal færdiggøres og godkendes af KCL. DPO'en har fremhævet dette i sine anbefalinger, hvorfor det skal prioriteres i 2021.
26	Implementering af passende sikkerhedsforanstaltninger (på baggrund af den foretagne risikovurdering)		Vi ligger meget lavt - og er gået tilbage på dette punkt i forhold til målingen for 2019, da vi er blevet over, at vi ikke foretager de fornødne risikovurderinger – og derved ikke kan implementere passende sikkerhedsforanstaltninger på baggrund heraf.
27	DPIA (konsekvensanalyse)/tærskelvurdering	Konsekvensanalyser er et kriterium, som afspejler et krav direkte efter GDPR. Konse-kvensanalyser handler om at sikre beskyttelse af persondata og beskytte borgernes rettigheder i forhold til behandlinger, som sandsynligvis vil indebære høje risici for borgernes rettigheder og frihedsrettigheder. Formålet med at gennemføre konsekvensanalyser er at reducere den høje risici, som en behandling måtte indebære.	Vi ligger meget lavt på dette punkt, da vi ikke har en procedure for konsekvensvurderinger og ikke har foretaget disse. Det er beskrevet i udkastet til procedure for risikovurdering, hvornår og hvordan der skal foretages en konsekvensvurdering. DPO'en har fremhævet dette i sine anbefalinger, hvorfor det bør prioriteres i 2021.
28	Sikkerhedstest	Kriteriet sikkerhedstest afspejler et krav direkte efter GDPR, hvorefter der skal gennemføres sikkerhedstest, som sikrer løbende afprøvning og vurdering af	Der arbejdes i dag ikke systematisk med processen om sikkerhedstests.

Nr.	Titel i rapport	Beskrivelse	Status
		implementerede sikkerhedsforanstaltningers effektivitet.	Den nuværende beredskabsplan er ikke ajourført, og det er i denne sikkerhedstest bør fremgå. DPO'en har fremhævet dette i sine anbefalinger, hvorfor det bør prioriteres i 2021.
29	Adgangsstyring til personoplysninger og systemer	Adgangsstyring til persondata er et kriterium, som afspejler et krav direkte efter GDPR, hvorefter organisationens ledere og medarbejdere kun må få adgang til de person-data (følsomme persondata) og systemer (systemer indeholdende følsomme person-data), som er nødvendige for udførelse af deres arbejdsopgaver.	Vi er gået frem i målingen i forhold til sidste år, og niveauet er acceptabelt.
30	Inddragelse af DPO	Det er et krav efter GDPR, at kommunen skal inddrage databeskyttelsesrådgiveren i alle spørgsmål vedrørende beskyttelse af persondata.	Vi har en procedure for inddragelse af DPO'en. Nøgletallene viser dog, at DPO'en kun er blevet inddraget i 1 ud af 6 indkøb af nye IT-systemer, hvilket ikke er tilfredsstillende. DPO'en har fremhævet dette i sine anbefalinger, hvorfor det bør prioriteres i 2021.
31	Privacy by design og privacy by default	Dette koncept handler om, at IT-systemer skal være sat op på en måde som sikrer, at medarbejderne kun kan tilgå de oplysninger, de skal bruge i deres arbejde. Dvs., at det ikke er tilstrækkeligt blot at have en log på systemet, så man kan tjekke, om en medarbejder har kigget på oplysninger, de ikke bør. Det må slet ikke være muligt at tilgå oplysninger, man ikke har brug for.	*Digitalisering og IT arbejder på at udarbejde IT arkitekturprincipper som et regelsæt til indkøb af IT-systemer. Her vil kravet om privacy by default og design indgå.* *Arkitekturprincipperne forventes at ligge klar i løbet af 2. halvår 2021*

Informationssikkerhed

Nr.	Titel i rapport	Beskrivelse	Status
32	Sikkerhedsprogram, ISO27001	Kriteriet afspejler det forhold, at implementering og drift af informationssikkerhed i en organisation forudsætter etablering af et sikkerhedsprogram.	Vi er gået tilbage i målingen på dette punkt i forhold til sidste år, da vi er blevet klar over, at vi ikke har et sikkerhedsprogram baseret på ISO27001.
33	Risikovurdering af kritiske forretningsprocesser, ISO27001	Kriteriet afspejler et princip efter ISO27001, hvorefter organisationen skal foretage risikovurdering og implementere sikkerhedsforanstaltninger for at bevare fortrolighed, integritet og tilgængelighed af in-formationsaktiver i organisationen.	Vi er gået tilbage i målingen på dette punkt i forhold til sidste år, da vi er blevet klar over, at vi ikke har et sikkerhedsprogram baseret på ISO27001.
34	Beredskabsplan	Kriteriet beredskabsplan afspejler et princip efter ISO27001, hvorefter der skal være en plan og procedure (beredskabsplan) i organisationen for videreførelse af kritiske forretningsprocesser i tilfælde af kritiske situationer (f.eks. ved omfattende hackerangreb).	Vi er gået tilbage på dette punkt i målingen, da vi ikke har en nedskrevet procedure for videreførelse af kritiske forretningsprocesser.
35	Test af beredskabsplan	Test af beredskabsplan er et kriterium, som afspejler et princip efter ISO27001, hvorefter der skal være en procedure i organisationen for afprøvning og forbedring af beredskabsplan gennem regelmæssig træning, afprøvning og evaluering, hvormed der sikres et effektivt beredskab. Uden test af beredskabsplan ved organisationen ikke, om en beredskabsplan virker efter hensigten i tilfælde af kritiske situationer.	Der er ikke en procedure for test af beredskabsplan.