DATABESKYTTELSESRÅDGIVERENS ÅRSRAPPORT 2020

,

Afsender:

Databeskyttelsesrådgiveren

Modtager:

Kommunalbestyrelsen i Ishøj Kommune

Indhold

Årsrapport 2020

Der er sket meget på databeskyttelsesområdet i 2020.

Kommunen lægger fortsat en stor arbejdsindsats i implementeringen af databeskyttelsesforordningens regler (herefter GDPR) og i driften i den forbindelse.

Det kan være en udfordring for kommunen at navigere i det databeskyttelsesretlige univers samtidig med, at kerneopgaverne skal løses. KL har i 2020 udgivet publikationen "GDPR – Benspænd" med eksempler fra landets kommuner, hvoraf flere har oplevet, at GDPR har givet udfordringer i løsningen af kerneopgaver. Datatilsynet har givet konkrete svar på benspænds eksemplerne, som viser, at GDPR ikke behøver at være et benspænd for kommunerne, men at reglerne er fleksible og kan tilpasses de mange forskellige situationer, hvor man behandler persondata. Det er vigtigt at huske, at reglerne er til for at sikre grundlæggende rettigheder om beskyttelse af persondata og retten til privatliv for borgere eller andre personer, som kommunen behandler oplysninger om. Beskyttelse af persondata og privatliv er en forudsætning for tillid til digitalisering i kommunen, og beskyttelsen skal derfor gå hånd i hånd med den øgede digitalisering, som allerede er i gang i kommunen, og de nye muligheder for yderligere digitalisering og brug af data, som følger med kommunernes nye digitaliseringsprogram 2021-2025.

Der er sket udvikling af bødepraksis hos Datatilsynet og retspraksis hos EU-Domstolen i 2020, som kommunen bør være opmærksom på.

Datatilsynet har indstillet en række kommuner til bøder for overtrædelse af GDPR. Gladsaxe og Hørsholm er blevet indstillet til bøder på henholdsvis 100.000 kr. og 50.000 kr. for ikke at beskytte persondata tilstrækkeligt. Lejre Kommune er indstillet til en bøde på 50.000 kr. for samme forseelse. Guldborgsund Kommune er blevet indstillet til en bøde på 50.000 kr. for et alvorligt brud på persondatasikkerheden.

EU-domstolen har afsagt en betydningsfuld dom (Schrems II), som har trukket en skarp linje for privatlivsbeskyttelse i situationer, hvor persondata overføres til USA eller andre usikre tredjelande (dvs. ikke EU-lande), hvor privatlivsbeskyttelsen ikke er på niveau med beskyttelsen i EU. Schrems II-dommen giver udfordringer, idet flere af kommunens systemer bygger på aftaler, som er indgået med databehandlere eller underdatabehandlere i USA.

Kommunen bør desuden være opmærksom på, at Storbritanniens udtrædelse af EU (Brexit) betyder, at det kan blive nødvendigt at tilpasse aftaler indgået med databehandlere i Storbritannien inden udgangen af juni 2021, hvor Storbritannien vil være et tredjeland.

Det er databeskyttelsesrådgiverens (herefter DPO'ens) opgave at rådgive kommunen om krav efter GDPR, at overvåge at kommunen overholder reglerne og at understøtte kommunen i at overholde reglerne.

I Ishøj Kommune har DPO'en udviklet værktøjer, som understøtter kommunens ansatte, når de skal løfte GDPR-opgaver, og udviklet og gennemført skræddersyet undervisning af kommunens ansatte. DPO'en har desuden rådgivet og vejledt kommunen ved forespørgsler. Derudover har DPO'en gennemført den årlige GDPR-modenhedsmåling, som måler på kommunens niveau og forudsætninger for overholdelse af GDPR. Endvidere har DPO'en gennemført en måling af overholdelsen af GDPR i Børn- og Ungeudvalget i Ishøj Kommune.

Denne årsrapport er den anden i rækken fra kommunens DPO og dækker perioden 1. januar 2020 – 31. december 2020.

Årsrapporten giver kommunens politiske ledelse en status for kommunens overholdelse af GDPR baseret på kommunens resultater for GDPR-modenhedsmålingen og kommunens egne oplyste tal for performance i forhold til udvalgte GDPR-områder (herefter kommunens GDPR-nøgletal). Desuden giver DPO'en anbefalinger til kommunens arbejde med databeskyttelse i 2021.

På side 4-9 giver DPO'en en status for kommunes overholdelse af GDPR samt anbefalinger og forslag til kontroller.

Bilag 1 indeholder de samlede resultater for GDPR-modenhedsmålingen, som DPO'en foretog i november 2020. Bilag 2 indeholder kommunens GDPR-nøgletal, som er indsamlet og opgjort i slutningen af 2020. Bilag 3 indeholder sagsstatistik for DPO'ens arbejde i perioden 1. januar 2020 – 31. december 2020.

Daniel Bach, DPO for Ishøj Kommune, 24. marts 2021.

Status for overholdelse af GDPR i kommunen

Resultater for GDPR-modenhedsmåling 2020

DPO'en gennemførte i november 2020 den årlige GDPR-modenhedsmåling, som måler på kommunens niveau og forudsætninger i forhold til at kunne overholde GDPR. Der er målt på 35 modenhedskriterier, som afspejler krav efter GDPR eller på anden måde har betydning for implementering af GDPR og drift af GDPR-opgaver i kommunen (fx ledelsesmæssig opbakning).

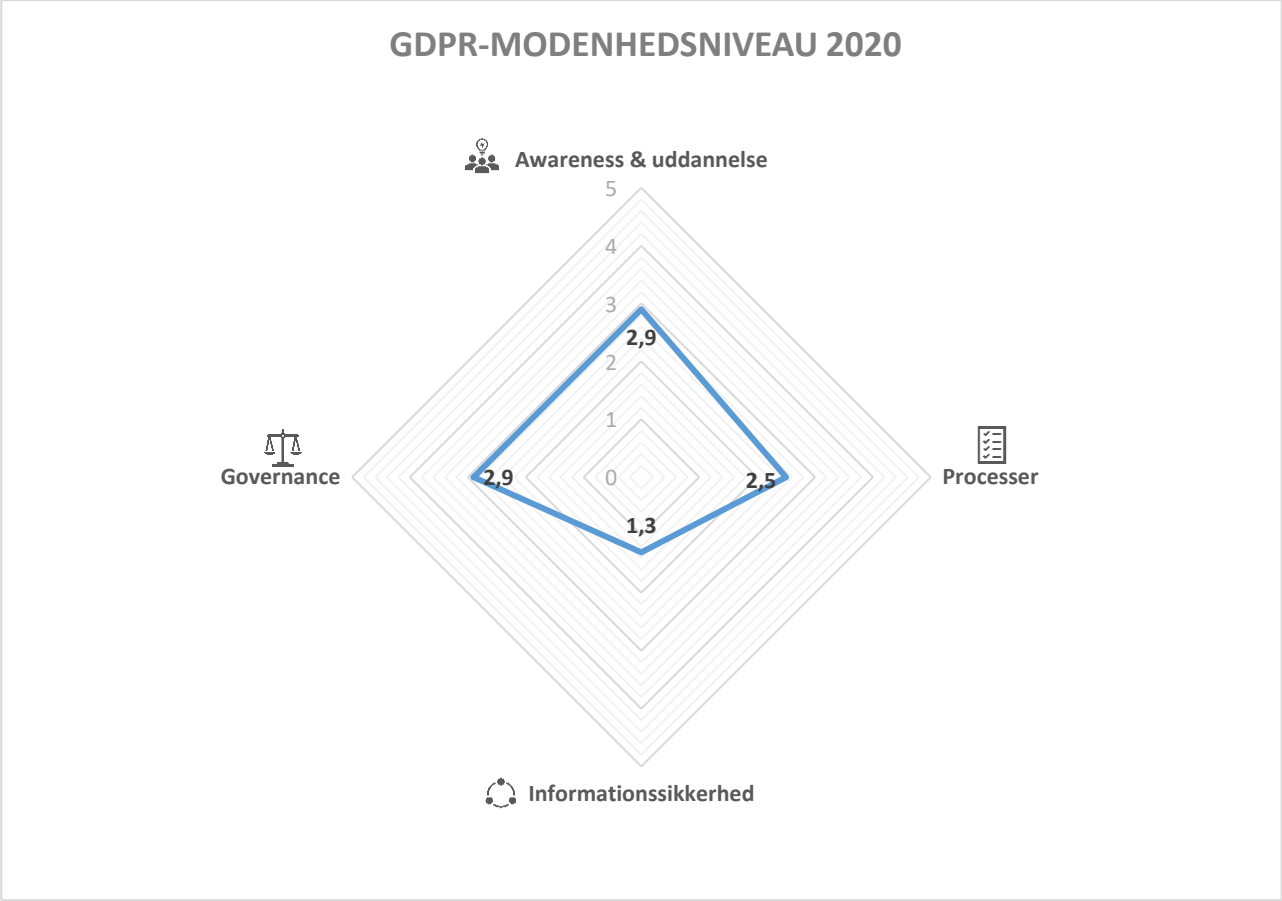
Målingen udgøres af besvarelser fra udpegede respondenter i kommunen (selvevaluering), og resultaterne udgør kommunens GDPR-modenhedsniveau for 2020.

Målestokken er baseret på følgende skala fra 1-5, som giver en indikation for overholdelse af GDPR (såkaldt GDPR-compliance). Kommunen bør som minimum stræbe efter modenhedsniveau 3 eller højere[1].

Modenhedsniveau	Beskrivelse	GDPR-compliance
1	Bevidst og planlagt, men ikke indført, ej dokumenteret (GDPR-compliance er ikke på plads).	👎
2	Delvist indført og dokumenteret (grundlag kan udnyttes som løftestang for GDPR-compliance).	👎
3	Indført og veldokumenteret (standardiseret tilgang til GDPR-compliance på plads).	👎
4	Implementeret i fuldt omfang (fuld standardiseret tilgang til GDPR-compliance på plads, herunder yderligere foranstaltninger (kontroller og opdatering eller opfølgning), som sikrer overholdelse af GDPR).	👍
5	Implementeret i fuldt omfang, optimering og forbedring af processer.	👍

[1] Det er som udgangspunkt ikke nødvendigt at være på modenhedsniveau 5 for at overholde GDPR eller have et tilfredsstillende modenhedsniveau med undtagelse af kriteriet om indgåelse af databehandleraftaler samt kriteriet om gennemførelse af tilsyn med databehandlere, hvor niveau 5 svarer til 100 % overholdelse af GPDR-krav.

Model 1: Gennemsnitsresultater for 2020 fordelt på fire hovedområder[2]



DPO'ens vurdering

Samlet set viser resultatet for GDPR-modenhedsmålingen i 2020, at kommunens GDPR-modenhedsniveau ligger under niveau 3 i forhold til mange kriterier for opfyldelse af GDPR-krav. Det indikerer, at der på tidspunktet for målingen er mange GDPR-krav, som kommunen ikke overholder. Det betyder, at der kan være risiko manglende eller utilstrækkelig beskyttelse af grundlæggende rettigheder for borgerne (persondatabeskyttelse og retten til privatliv), ligesom der kan være risiko for, at kommunen kan få kritik eller bøder fra Datatilsynet, hvis tilsynet skulle undersøge kommunens overholdelse af GDPR-krav på de pågældende områder.

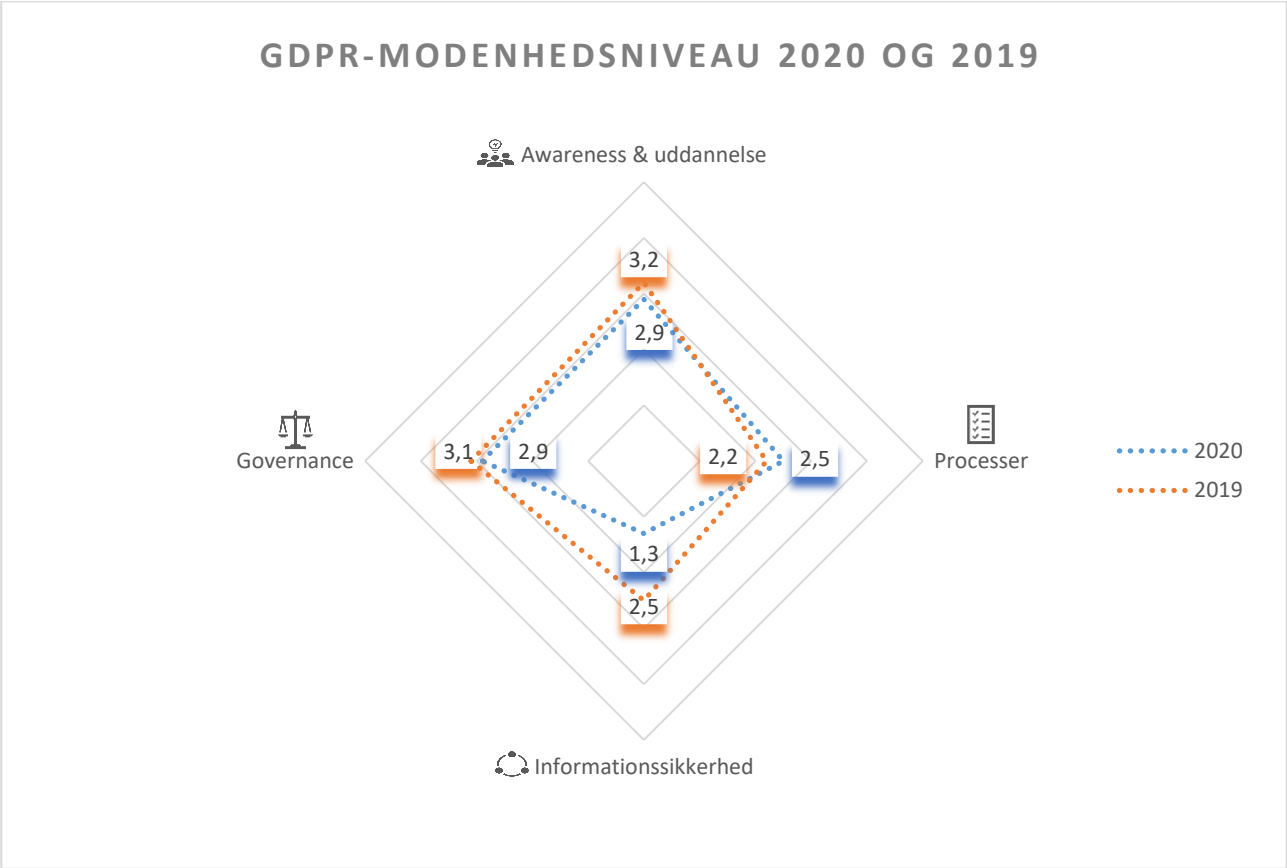
Kommunens gennemsnitlige GDPR-modenhedsniveau i 2020 er 2,4, og modenheden er dermed faldet med 0,1 sammenlignet med målingen i 2019, hvor gennemsnitsniveauet var 2,5. Selvom kommunens gennemsnitlige modenhedsniveau er faldet en anelse, viser de enkelte resultater for målingen i 2020 dog, at kommunen faktisk har rykket sig på de punkter, kommunen har fokuseret på. Kommunens indsats har således udmøntet sig i målbare resultater, og kommunen har taget et skridt i den rigtige retning i forhold til overholdelse af en række GDPR-krav. Omvendt viser det forhold, at kommunen fortsat ligger under niveau 3 i forhold til mange kriterier, herunder at kommunens modenhedsniveau er faldet for en række kriterier[3], at der fortsat er lang vej for kommunen mod overholdelse af alle GDPR-krav.

---

[2] Se bilag 1 for en oversigt over de 35 kriterier og deres indplacering i de fire hovedområder.

[3] Kommunen har oplyst, at nedgangen i modenhedsniveauet for kriterierne under hovedområdet governance samt awareness og uddannelse skyldes, at der ikke har været nogen aktiviteter, som

Model 2: Resultat af GDPR-modenhedsmåling i 2020 sammenlignet med målingen i 2019[4]



Kommunens GDPR-nøgletal 2020

Henvendelser fra borgere

Kommunen har modtaget 11 henvendelser fra borgere, som har gjort brug af deres rettigheder efter GDPR i 2020. Det er et fald sammenlignet med 2018/19, hvor kommunen modtog 40 henvendelser. Kommunen har håndteret stort set alle henvendelserne (10 ud af 11) inden for 30-dagesfristen efter tidspunktet for modtagelsen af anmodningen.

Det er generelt DPO'ens vurdering, at kommunen har håndteret henvendelserne i overensstemmelse med GDPR.

Brud på persondatasikkerheden

Kommunen har registreret 43 brud på persondatasikkerheden i 2020. Det er en stigning sammenlignet med 2018/19, hvor kommunen registrerede 32 brud på persondatasikkerheden. I 29 ud af de i alt 43 brud i 2020 har kommunen foretaget anmeldelse til Datatilsynet, hvoraf alle brud er anmeldt til Datatilsynet inden for den rette frist, dvs. inden 72 timer efter kommunen har fået kendskab til bruddet. Dette er en forbedring sammenlignet med 2018/19, hvor kommunen foretog anmeldelse inden for den rette frist i 20 ud af 22 brud, som blev anmeldt til Datatilsynet. Kommunen har i 14 ud af de 29 brud, som er anmeldt til Datatilsynet i 2020, foretaget

---

kan begrunde opretholdelsen af niveauerne for de pågældende kriterier, der blev vurderet lavere i 2020. Herudover har kommunen oplyst, at nedgangen i modenhedsniveaet for kriterierne under hovedområdet informationssikkerhed skyldes, at kommunen er blevet klogere på, hvad kravene efter GDPR og informationssikkerhed faktisk er, hvilket afspejles i de lavere vurderede niveauer i 2020.

[4] Der henvises til bilag 1 for de samlede resultater for GDPR-modenhedsmålingerne i 2020 og 2019.

underretning af de borgere, der har været udsat for brud på sikkerheden ved kommunens behandling af deres persondata.

Det er positivt, at kommunen er blevet bedre til at anmelde brud til Datatilsynet inden for den rette frist. Det er generelt DPO'ens vurdering, at kommunen har håndteret brud på persondatasikkerheden i overensstemmelse med GDPR.

Nye it-løsninger og inddragelse af DPO'en
Kommunen har anskaffet 6 nye it-løsninger til brug for behandling af persondata i 2020, hvoraf DPO'en er blevet inddraget i 1 tilfælde.

Det er DPO'ens vurdering, at kommunens inddragelse af DPO'en i forhold til anskaffelse af nye it-løsninger er utilstrækkelig. Kommunen bør spørge DPO'en til råds i langt flere tilfælde, hvor kommunen påtænker at anskaffe it-løsninger til brug for behandling af persondata. Dette gælder også, før kommunen eventuelt offentliggør udbudsmateriale, hvor kommunen skal stille krav til løsningerne og skal tage højde for privacy by design. Systemer til brug for behandling af persondata skal fra start være designet således, at krav efter GDPR kan overholdes, og persondata kan beskyttes, og der er en betydelig ressourcebesparelse ved at indtænke GDPR så tidligt som muligt sammenlignet med det ressourcetræk, der kan være forbundet med efterfølgende at skulle rette op og tilpasse løsninger mv. Hertil kommer den retssikkerhedsmæssige værdi for borgere, hvis oplysninger kommunen skal behandle i disse systemer.

Risikostyring
Kommunen har gennemført 1 risikovurdering[5] i forhold til behandling af persondata, men har hverken gennemført tærskelvurderinger[6] eller konsekvensanalyser vedrørende databeskyttelse[7] i 2020.

Det er DPO'ens vurdering, at det er utilstrækkeligt kun at gennemføre 1 risikovurdering, når der henses til det store omfang af persondata og karakteren af persondata (følsomme og fortrolige data) i kommunen, herunder antallet af nye it-løsninger til brug for behandling af persondata i kommunen. Risikostyring er en central komponent i en risikobaseret tilgang til GDPR, som forudsætter løbende risikovurderinger i forhold til persondatabehandling og implementering af passende sikkerhedsforanstaltninger, hvis risiciene for persondata er for høj. Uden risikovurderinger er det ikke muligt at vurdere, om der er en passende beskyttelse af persondata. Beskyttelse af persondata og privatlivet er en forudsætning for tillid til digitalisering i kommunen, og beskyttelsen skal derfor gå hånd i hånd med den øgede digitalisering, som allerede er i gang i kommunen, og de nye muligheder for yderligere digitalisering og brug af data. Kommunen

[5] Risikovurderinger skal afdække, hvilke risici for brud på borgernes rettigheder (rettigheder efter GDPR) og frihedsrettigheder (ret til privat liv og ret til databeskyttelse) som er forbundet med behandling af persondata i kommunen fx risici forbundet med behandling af persondata i it-systemer på skoleområdet.

[6] Tærskelvurderinger skal identificere om planlagte nye behandlinger af persondata i kommunen sandsynligvis indebærer en høj risiko for brud på borgernes rettigheder og frihedsrettigheder og derfor kræver udarbejdelse af en konsekvensanalyse vedrørende databeskyttelse forud for behandling af persondata fx er behandlingstyper i Datatilsynets positivliste over behandlingsaktiviteter pr. definition underlagt kravet om en konsekvensanalyse.

[7] Konsekvensanalyser vedrørende databeskyttelse skal hvis påkrævet gennemføres forud for behandling af persondata og skal som minimum omfatte en beskrivelse af formål for behandling, en vurdering af proportionalitet og nødvendighed, en risikovurdering samt foranstaltninger for at nedbringe høj risiko (alt sammen for at sikre overholdelse af borgernes rettigheder og frihedsrettigheder forinden behandling af persondata).

bør derfor gennemføre flere risikovurderinger af persondatabehandling med henblik på at sikre en passende beskyttelse af borgernes persondata.

Det er desuden DPO'ens vurdering, at det forekommer utilstrækkeligt, at kommunen ikke har gennemført tærskelvurderinger. Uden tærskelvurderinger kan kommunen ikke identificere, om planlagte nye behandlinger af persondata i kommunen vil indebære en høj risiko for brud på borgernes rettigheder og frihedsrettigheder. Det betyder, at kommunen ikke kan identificere, om planlagte nye behandlinger af persondata i kommunen er underlagt krav om gennemførelse af en konsekvensanalyse vedrørende databeskyttelse forud for behandling af persondata.

Tilsyn fra Datatilsynet og intern kontrol med overholdelse af GDPR
Datatilsynet har iværksat 1 tilsyn af kommunen vedrørende behandling af persondata i Ishøj Svømmehal. Tilsynssagen er verserende hos Datatilsynet. I 2 tilfælde har Datatilsynet fulgt op over for kommunen og bedt om en uddybning vedrørende brud på persondatasikkerheden i kommunen, hvorefter Datatilsynet har lukket opfølgningssagerne. Kommunen har ikke gennemført interne kontroller med overholdelse af GDPR i 2020.

Det er DPO'ens vurdering, at det er utilstrækkeligt, at kommunen ikke har gennemført interne kontroller med overholdelse af GDPR. Det er et krav, at kommunen løbende skal tjekke overholdelsen af GDPR med interne kontroller. Kommunen bør udvikle et koncept og en årlig plan for stikprøvekontrol efter en risikobaseret tilgang og gennemføre stikprøvekontroller for at sikre kommunens GDPR-compliance.

Kommunens GDPR-ressourcer
Kommunen har 1 årsværk dedikeret til arbejdet med GDPR, og kommunen bruger derudover 0,5 årsværk fordelt på enkelte medarbejdere på GDPR-arbejdet[8]. Antal årsværk i 2020 til GDPR er opnormeret med 0,5 årsværk sammenlignet med 2018/19.

Selvom antal årsværk er opnormeret, bør kommunen alligevel overveje, om de nuværende ressourcer er tilstrækkelige til at udvikle en risikobaseret tilgang til GDPR (se afsnittet ovenfor om risikostyring).

Der henvises til bilag 2 for en gennemgang af kommunens GDPR-nøgletal.

DPO'ens anbefaling samt forslag til kontrol

DPO'ens anbefaling på baggrund af kommunens GDPR-nøgletal 2020 og GDPR-modenhedsmåling 2020	Forslag til kontrol
• Årshjul for GDPR-arbejdsopgaver - baseret på resultat for GDPR-modenhedsmåling: 2	Etablere et årshjul for GDPR-arbejdsopgaver som fundament til gennemførelse af løbende GDPR-opgaver centralt og decentralt i kommunen.

[8] Kommunen har supplerende oplyst, at der herudover er andre medarbejdere centralt og decentralt, som har deltaget i GDPR-arbejdet i 2020, uden at dette er blevet tidsregistreret. Ishøj Kommune er herudover omfattet af DPO-funktionen i Den Storkøbenhavnske Digitaliseringsforening, herunder tilsynsfunktionen i Den Storkøbenhavnske Digitaliseringsforening, som fører tilsyn med fælles databehandlere for kommunerne i Den Storkøbenhavnske Digitaliseringsforening. Kommunen kanaliserer ressourcer til DPO-funktionen svarende til 1/5 af et årsværk samt ressourcer til tilsynsfunktionen svarende til 1/11 af et årsværk.

• Nye it-løsninger og inddragelse af DPO'en - baseret på kommunens GDPR-nøgletal.	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.
• Register for databehandlere – baseret på modenhedsmåling: 	Etablere et centralt register for databehandlere, som afspejler status for databehandleraftale, risici, tilsynsstatus og eventuelle kritiske mangler samt bruge registreret som et prioriterings- og styringsværktøj til kommunens tilsyn med *egne* databehandlere[9] baseret på risici forbundet med persondatabehandling.
• Procedure for tilsyn med databehandlere – baseret på modenhedsmåling: 	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 Den Storkøbenhavnske Digitaliseringsforening samt udarbejde tilsynserklæringer om tilsynsrapporter fra tilsynsfunktionen.
• Gennemførelse af tilsyn med databehandlere – baseret på modenhedsmåling: 	Gennemføre flere tilsyn med *egne* databehandlere på baggrund af en plan for tilsyn, herunder faktisk gennemgå tilsynsrapporter fra tilsynsfunktionen i Den Storkøbenhavnske Digitaliseringsforening samt udarbejde tilsynserklæringer om tilsynsrapporter fra tilsynsfunktionen.
○ Risikostyring • Risikovurderinger efter GDPR - baseret på kommunens GDPR-nøgletal samt resultat for modenhedsmåling: 	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.
○ Risikostyring • Implementering af passende sikkerhedsforanstaltninger – baseret på kommunens GDPR-nøgletal samt resultat for modenhedsmåling: 	Etablere en proces, der sikrer, at kommunen på baggrund af risikovurderinger efter GDPR implementerer passende sikkerhedsforanstaltninger for beskyttelse af persondata, hvis risiko for persondata er for høj (risikohåndtering).

[9] Med kommunens *egne* databehandlere menes Ishøj Kommunes databehandlere, som ikke er omfattet af tilsynsfunktionen i Den Storkøbenhavnske Digitaliseringsforening, som fører tilsyn med fælles databehandlere for kommunerne i Den Storkøbenhavnske Digitaliseringsforening.

○ Risikostyring • Sikkerhedstest – baseret på resultat for modenhedsmåling: 	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.
○ Risikostyring • Tærskelvurderinger – baseret på kommunens GDPR-nøgletal samt resultat for modenhedsmåling: 	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.
• Intern kontrol med overholdelse af politikker for databeskyttelse og GDPR i kommunen - baseret på kommunens GDPR-nøgletal samt resultat for modenhedsmåling: 	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).

Bilag 1

GDPR-modenhedsmåling 2020

Formål

GDPR-modenhedsmålingen af kommunen i november 2020 blev udført som en del af DPO'ens lovpligtige opgave med at overvåge kommunens overholdelse af GDPR.

Formålet er at måle kommunens niveau og forudsætninger for overholdelse af GDPR samt at skabe læring og understøtte kommunen i arbejdet med implementering af GDPR og drift af GDPR-opgaver.

På side 12-24 vises de samlede resultater for GDPR-modenhedsmålingen i 2020 med blå søjler. For sammenligningens skyld gengives resultaterne for 2019 med orange søjler.

Metode

Målingen af GDPR-modenheden er baseret på principper fra den anerkendte AICPA Privacy Maturity Model[10]. DPO'en har modificeret modellens kriterier til kommunal kontekst med primært fokus på GDPR. Data, som ligger til grund for resultaterne i målingen, er baseret på en survey med svar fra respondenter, som kommunen internt har udpeget (selvevaluering).

For at sikre kvalitet i de indsamlede data har DPO'en gennemført workshops for de udpegede respondenter, hvor respondenterne har haft mulighed for at besvare surveyen, og hvor DPO'en har guidet respondenterne gennem modenhedskriterierne og besvaret spørgsmål mv.

For hvert modenhedskriterie spørges der til niveau for opfyldelse af krav efter GDPR eller andre forhold af betydning for GDPR og informationssikkerhed. Hvert kriterie indeholder fem udsagn (svarende til modenhedsniveau 1-5) med beskrivelse af aktiviteter, dokumentation, procedurer og andre oplysninger. Respondenterne er instrueret i at vælge det udsagn, som er mest retvisende i forhold til det det nuværende GDPR-modenhedsniveau i kommunen. Respondenternes valg af udsagn definerer GDPR-modenhedsniveauet for hvert målte kriterie. DPO'en har verificeret respondenternes besvarelser af surveyen, hvis det er skønnet relevant.

Omfang

GDPR-modenhedsmålingen omfatter dels en måling på baggrund af en række kriterier i en afdeling i kommunen, som har ansvar for tværgående mål, rammer og foranstaltninger, som omfattes af GDPR. Og dels en måling på baggrund af andre kriterier i hver af kommunens udpegede fagområder, som har ansvar for overholdelse af reglerne i GDPR.

Modenhedskriterier

Kriterierne er indplaceret under følgende fire hovedområder (kriterier med * afspejler krav direkte efter GDPR):

Governance

1. Ledelsesmæssig understøttelse
2. Roller og ansvar*
3. Politikker for beskyttelse af persondata*
4. Opdatering af politikker for beskyttelse af persondata*
5. Formidling af politikker for beskyttelse af persondata
6. Intern kontrol med overholdelse af politikker og GDPR-compliance *
7. Årshjul for GDPR-arbejdsopgaver

Awareness og uddannelse

[10] The American Institute of Certified Public Accountants (AICPA).

8. Awareness*
9. Uddannelse*

Processer

10. Fortegnelse*
11. Indsamling til sagligt formål (dataminimering)*
12. Datakvalitet*
13. Formålsbegrænsning*
14. Opbevaringsbegrænsning*
15. Gyldigt samtykke efter GDPR*
16. Oplysningspligt*
17. Håndtering af anmodninger fra borgere, som gør brug af deres rettigheder efter GDPR*
18. Håndtering af brud på persondatasikkerheden*
19. Register for databehandlere*
20. Kvalitetssikring af databehandlere (due diligence)*
21. Kvalitetssikring af databehandleraftaler*
22. Indgåelse af databehandleraftaler*
23. Procedure for tilsyn med databehandlere*
24. Tilsyn med databehandlere*
25. Risikovurderinger efter GDPR*
26. Implementering af sikkerhedsforanstaltninger*
27. Konsekvensanalyse vedrørende databeskyttelse og tærskelvurdering*
28. Sikkerhedstest*
29. Adgangsstyring til persondata*
30. Inddragelse af DPO'en*
31. Privacy by design og privacy by default*

Informationssikkerhed

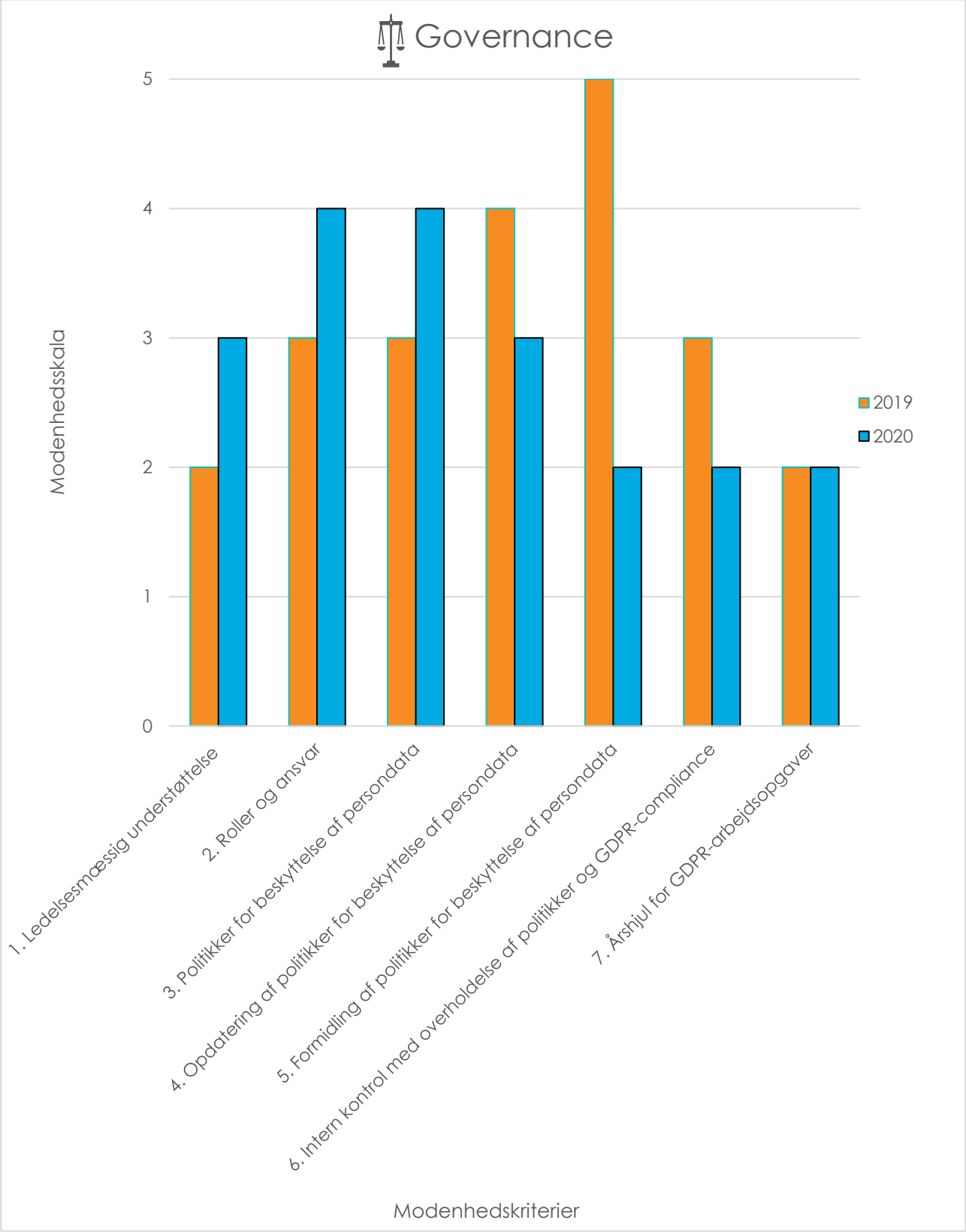
32. Sikkerhedsprogram (ISO27001)
33. Risikovurderinger af kritiske forretningsprocesser (ISO27001)
34. Beredskabsplan
35. Test af beredskabsplan

Målestok

Modenhedsniveau	Beskrivelse	GDPR-compliance
1	Bevidst og planlagt, men ikke indført, ej dokumenteret. (GDPR-compliance er ikke på plads).	👎
2	Delvist indført og dokumenteret (Grundlag kan udnyttes som løftestang for GDPR-compliance).	👎
3	Indført og veldokumenteret (Standardiseret tilgang til GDPR-compliance på plads).	👎
4	Implementeret i fuldt omfang (Fuld standardiseret tilgang til GDPR-compliance på plads, herunder yderligere foranstaltninger (kontroller og opdatering eller opfølgning), som sikrer overholdelse af GDPR).	👍
5	Implementeret i fuldt omfang, optimering og forbedring af processer.	👍

Ikonerne i højre kolonne ovenfor skal ses i lyset af, at GDPR-modenhedsmålingen ikke er baseret på DPO'ens vurdering af skriftlig dokumentation fra kommunen, men på en selvevaluering af udpegede respondenter fra kommunen.

Governance


Governance
5
4
3
2
1
0
Modenhedsskala
2019
2020
1. Ledelsesmæssig understøttelse
2. Roller og ansvar
3. Politikker for beskyttelse af persondata
4. Opdatering af politikker for beskyttelse af persondata
5. Formidling af politikker for beskyttelse af persondata
6. Intern kontrol med overholdelse af politikker og GDPR-compliance
7. Årshjul for GDPR-arbejdsopgaver
Modenhedskriterier

Introduktion til governance

Governance (styring og ledelse) forudsætter, at ledelsen "sætter tonen" i forhold GDPR-compliance i kommunen. Roller og ansvar for GDPR-compliance skal være tydeligt defineret. Politikker for beskyttelse af persondata skal implementeres, opdateres og bør formidles til medarbejdere og ledere. Og der skal ske opfølgning (intern kontrol) med, om politikker for beskyttelse af persondata og GDPR overholdes i kommunen. Sidst men ikke mindst bør der være årshjul, som definerer, hvilke GDPR-arbejdsopgaver, der skal udføres. Kriterierne under governance afspejler krav direkte efter GDPR bortset fra kriterierne om ledelsesmæssig understøttelse, formidling af politikker for beskyttelse af persondata samt årshjul for GDPR-arbejdsopgaver.

1. Ledelsesmæssig understøttelse

Kriteriet afspejler det forhold, at ledelsesmæssigt engagement og understøttelse er en forudsætning for implementering og drift af GDPR i kommunen (ledelsen "sætter tonen" i forhold til GDPR-compliance i kommunen). Der er målt på, om direktion og ledelse understøtter GDPR-compliance ved at kommunikere klart og tydeligt i kommunen om vigtigheden af at overholde GDPR.

Resultat 2020:

2. Roller og ansvar

Kriteriet afspejler det forhold, at roller og ansvar skal være defineret i kommunen i forhold til implementering og driftsopgaver. Der er målt på, om roller og ansvar for GDPR-compliance er tydeligt defineret.

Resultat 2020:

3. Politikker for beskyttelse af persondata

Kriteriet afspejler det forhold, at der skal være interne politikker i kommunen, som beskriver, hvordan ledere og medarbejdere skal håndtere og beskytte persondata i kommunen. Der er målt på, om kommunen har interne politikker for håndtering og beskyttelse af persondata.

Resultat 2020:

4. Opdatering af politikker for beskyttelse af persondata

Kriteriet afspejler det forhold, at der periodisk skal foretages en vurdering af, om der er behov for at opdatere kommunens politikker for beskyttelse af persondata. Der er målt på, om der er allokeret ansvar for periodisk opdatering af politikker for beskyttelse af persondata.

Resultat 2020:

5. Formidling af politikker for beskyttelse af persondata

Kriteriet afspejler det forhold, at formidling af kommunens politikker for beskyttelse af persondata til kommunens medarbejdere og ledere er en forudsætning for at sikre kendskab til politikkerne. Der er målt på, om politikker for beskyttelse af persondata kommunikeres til medarbejdere og ledere.

Resultat 2020:

6. Intern kontrol med overholdelse af politikker og GDPR-compliance

Kriteriet afspejler det forhold, at kommunen skal foretage intern kontrol med, om politikker for beskyttelse af persondata og GDPR overholdes i kommunen for at sikre GDPR-compliance. Der er målt på, om der er allokeret ansvar i kommunen for løbende kontrol med overholdelse af politikker og GDPR, herunder om der er allokeret ansvar for opfølgning i tilfælde af manglende overholdelse af politikker og GDPR.

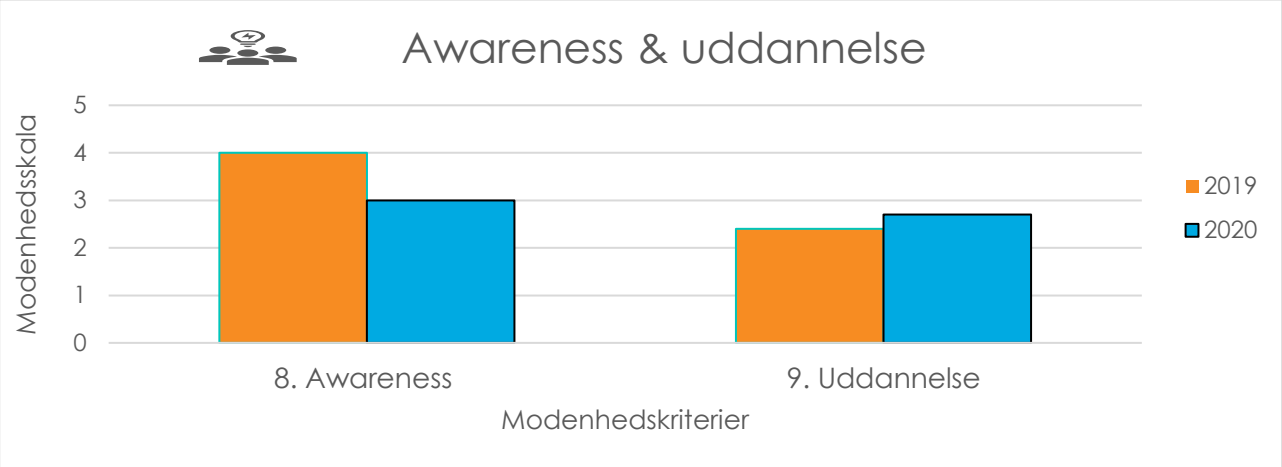
Resultat 2020:

7. Årshjul for GDPR-arbejdsopgaver

Kriteriet afspejler det forhold, at et årshjul er et relevant værktøj, som kan understøtte kommunen i forhold til udførelse af faste GDPR-aktiviteter i kommunen (fx risikovurderingsaktiviteter, awareness- og uddannelsesaktiviteter, opfølgning (kontrol) med, om politikker for beskyttelse af persondata og GDPR overholdes i kommunen og tilsyn med databehandlere).

Resultat 2020:

Awareness & uddannelse



Introduktion til awareness og uddannelse

Det følger af GDPR, at der skal være viden og opmærksomhed (awareness) hos medarbejdere og ledere omkring beskyttelse af persondata, og at medarbejdere og ledere, som medvirker i behandling af persondata, skal trænes i beskyttelse af persondata og overholdelse af GDPR (uddannelse). Kriterierne under hovedområdet awareness og uddannelse afspejler krav direkte efter GDPR.

8. Awareness

Kriteriet afspejler det forhold, at der skal være viden og opmærksomhed hos medarbejdere og ledere omkring beskyttelse af persondata. Der er målt på, om medarbejdere og ledere løbende informeres om beskyttelse af persondata med henblik på at skabe opmærksomhed og varsomhed i forhold til persondatabeskyttelse i kommunen.

Resultat 2020:

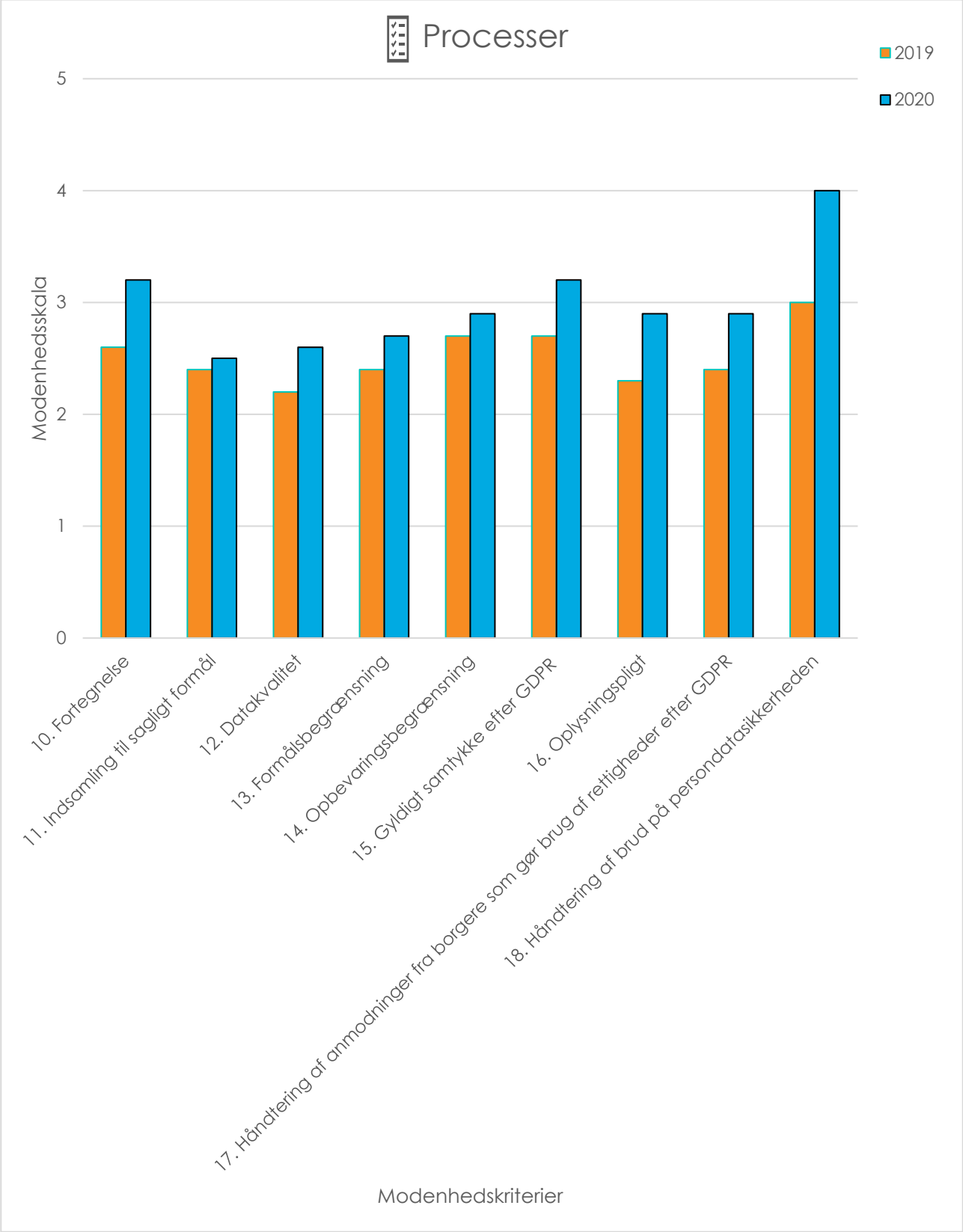
9. Uddannelse

Kriteriet afspejler det forhold, at medarbejdere og ledere, som medvirker i behandling af persondata, skal trænes i beskyttelse af persondata og overholdelse af GDPR. Der er målt på, om medarbejdere og ledere i kommunens fagområder/enheder løbende trænes (fx kurser, oplæring eller online-undervisning) i overholdelse af GDPR og beskyttelse af persondata.

Resultat 2020:

(her gennemsnit af fagområdernes/enhedernes besvarelser).

Processer



Introduktion til processer

Det følger af ansvarlighedsprincippet (accountability) efter GDPR, at der skal foreligge processer og dokumentation for overholdelse af GDPR. Det betyder, at der bl.a. skal være fortegnelser over behandlinger af persondata i kommunen, nedskrevne procedurer som sikrer, at kommunen kan overholde god databehandlerskik (behandlingsprincipper efter GDPR) og en lang række øvrige GDPR-krav, som kommunen er underlagt (bl.a. risikovurderinger, tærskelvurderinger, konsekvensanalyser vedrørende databeskyttelse og tilsyn med databehandlere). Alle kriterierne under processer afspejler krav direkte efter GDPR.

10. Fortegnelse

Kriteriet afspejler det forhold, at der skal føres en skriftlig fortegnelse over behandlinger af persondata (såkaldte behandlingsaktiviteter) i kommunen. Der er målt på, om der i kommunens enheder/fagområder føres en skriftlig fortegnelse over behandlingsaktiviteter.

Resultat 2020:

(her gennemsnit af fagområdernes/enhedernes besvarelser).

Behandlingsprincipperne efter GDPR

Det følger af GDPR, at enhver behandling af persondata i kommunen skal være i overensstemmelse med behandlingsprincipperne efter GDPR. Behandlingsprincipperne handler grundlæggende om, at kommunen kun må indsamle persondata til sagligt formål, at persondata skal være korrekte, at behandling af persondata skal begrænses til det formål, hvortil persondata er blevet indsamlet (formålsbegrænsning), og at persondata ikke må opbevares i længere tid end nødvendigt af hensyn til det formål, hvortil persondata behandles (opbevaringsbegrænsning). Kommunen skal kunne påvise overholdelsen af behandlingsprincipperne, jf. ansvarlighedsprincippet, hvilket i udgangspunktet forudsætter dokumentation i form af nedskrevne procedurer, som sikrer overholdelsen af behandlingsprincipperne i kommunen. I GDPR-modenhedsmålingen er der i enhederne/fagområderne målt på, om der foreligger nedskrevne procedurer, som sikrer, at behandlingsprincipperne kan overholdes i forbindelse med behandlingen af persondata.

11. Indsamling til sagligt formål (dataminimering)

Kriteriet afspejler det forhold, at kommunen skal sikre (ved nedskrevne procedurer), at der kun indsamles persondata til sagligt formål, og at der kun indsamles persondata, som er nødvendig af hensyn til formålet. Der er målt på, om der er i kommunens enheder/fagområder er en nedskrevet procedure, der sikrer, at princippet kan overholdes.

Resultat 2020:

(her gennemsnit af fagområdernes/enhedernes besvarelser).

12. Datakvalitet

Kriteriet afspejler det forhold, at kommunen skal sikre (ved nedskrevne procedurer), at de behandlede persondata er korrekte, og at persondata, som måtte være fejlagtige, rettes eller slettes straks. Der er målt på, om der er i kommunens enheder/fagområder er nedskrevet procedure, der sikrer, at princippet kan overholdes).

Resultat 2020:

(her gennemsnit af fagområdernes/enhedernes besvarelser).

13. Formålsbegrænsning

Kriteriet afspejler forholdet, at kommunen skal sikre (ved nedskrevne procedurer), at persondata ikke behandles (viderebehandles/genbruges) på en måde, som er uforenelig med det formål, hvortil persondata i første omgang blev indsamlet. Der er målt på, om der er i kommunens enheder/fagområder er en nedskrevet procedure, der sikrer, at princippet kan overholdes.

Resultat 2020:

(her gennemsnit af fagområdernes/enhedernes besvarelser).

Det skal bemærkes, at det kun er nødvendigt med en nedskrevet procedure om formålsbegrænsning i områder i kommunen, hvor der faktisk sker behandling af persondata til et andet formål end det, hvortil persondata blev indsamlet i første omgang.

14. Opbevaringsbegrænsning

Kriteriet afspejler det forhold, at kommunen (ved nedskrevne procedurer) skal sikre, at persondata ikke opbevares i længere tid end nødvendigt for opfyldelse af det formål, som persondata i første omgang blev indsamlet til. Der er målt på, om der er i kommunens enheder/fagområder er en nedskrevet procedure, der sikrer, at princippet kan overholdes.

Resultat 2020:

(her gennemsnit af fagområdernes/enhedernes besvarelser).

15. Gyldigt samtykke efter GDPR

Kriteriet afspejler det forhold, at behandling af persondata, som er sker på baggrund af samtykke fra borgere til, at kommunen må indsamle og behandle deres persondata, skal være et gyldigt samtykke efter GDPR. Der er målt på, om der i enheder/fagområder, som har besvaret bekræftende på, at de behandler persondata på baggrund af samtykke efter GDPR, er en nedskrevet procedure, som sikrer, at der kan indhentes gyldigt samtykke efter GDPR, før indsamling og behandling af persondata.

Resultat 2020:

(her gennemsnit af fagområdernes/enhedernes besvarelser).

16. Oplysningspligt

Kriteriet afspejler det forhold, at borgere (og andre personer), som kommunen behandler persondata om, skal orienteres skriftligt om behandlingsformål og behandlingshjemmel og øvrige forhold i forbindelse med kommunens første indsamling af persondata om vedkommende. Der er målt på, om der i kommunens fagområder/enheder er en nedskrevet procedure, som sikrer, at der kan udleveres skriftlige oplysninger til borgerne og andre, som der indsamles og behandles persondata om.

Resultat 2020:

(her gennemsnit af fagområdernes/enhedernes besvarelser).

17. Håndtering af anmodninger fra borgere, som gør brug af rettigheder efter GDPR

Kriteriet afspejler det forhold, at kommunen rettidigt skal håndtere henvendelser fra borgere (og andre personer), som kommunen behandler persondata, som gør brug af deres rettigheder efter GDPR (fx indsigt i egne persondata). Der er målt på, om der i kommunens enheder/fagområderne er en nedskrevet procedure, som sikrer håndtering af henvendelser fra borgere, som gør brug af deres rettigheder efter GDPR.

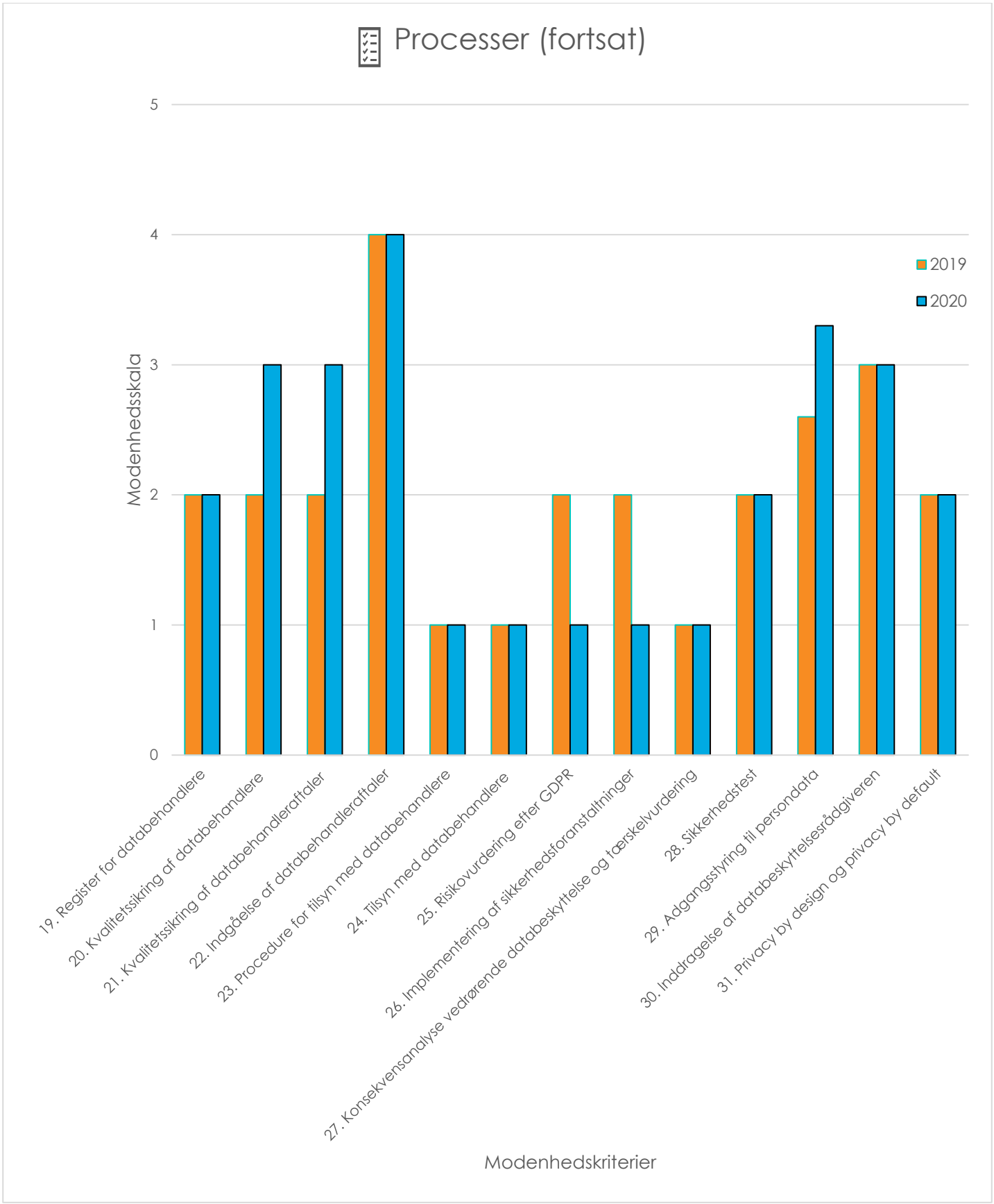
Resultat 2020:

(her gennemsnit af fagområdernes/enhedernes besvarelser).

18. Håndtering af brud på persondatasikkerheden

Kriteriet afspejler det forhold, at brud på persondatasikkerheden skal registreres i kommunen og i de fleste tilfælde anmeldes til Datatilsynet, ligesom de borgere (og andre personer), hvis persondata der er genstand for bruddet, i nogle tilfælde skal underrettes af kommunen. Der er målt på, om der i kommunen er en nedskrevet procedure, der sikrer en central håndtering og registrering af brud på persondatasikkerheden.

Resultat 2020:



19. Register for databehandlere

Kriteriet afspejler det forhold, at der skal være et register over databehandlere i kommunen, for at kommunen kan føre tilsyn med databehandlere. Der er målt på, om

der i kommunen er etableret et centralt register for alle databehandlere i kommunen.

Resultat 2020:

20. Kvalitetssikring af databehandlere (due diligence)

Kriteriet afspejler det forhold, at kommunen kun må benytte databehandlere, som kan stille de fornødne garantier for, at de vil og kan gennemføre passende sikkerhedsforanstaltninger, som sikrer passende beskyttelse af persondata. For at overholde dette krav skal kommunen foretage en kvalitetssikring (fx gennemføre en questionnaire) af databehandlere, før der indgås en databehandleraftale med databehandlere. Der er målt på, om der i kommunen er etableret en nedskrevet procedure, som sikrer, at kommunen kan kvalitetssikre databehandlere, inden der indgås en databehandleraftaler.

Resultat 2020:

21. Kvalitetssikring af databehandleraftaler

Kriteriet afspejler det forhold, at databehandleres behandling af persondata for kommunen altid skal ske i henhold til en gyldig databehandleraftale, som er i overensstemmelse med GDPR. Der er målt på, om der foreligger en nedskrevet procedure, som sikrer, at databehandlerens behandling af persondata for kommunen altid sker i henhold til en gyldig databehandleraftale.

Resultat 2020:

22. Indgåelse af databehandleraftaler

Kriteriet afspejler det forhold, at kommunen skal indgå databehandleraftaler med alle databehandlere, som behandler persondata på vegne af kommunen. Der er målt på, om kommunen har indgået databehandleraftaler med sine databehandlere (målt procentvist)[11].

Resultat 2020:

23. Procedure for tilsyn med databehandlere

Kriteriet afspejler det forhold, at der skal være en nedskrevet procedure, som sikrer, at kommunen kan føre tilsyn sine databehandleres opfyldelse af databehandleraftalernes betingelser samt implementering og opretholdelse af passende foranstaltninger for beskyttelse af persondata. Der er målt på, om der foreligger en nedskrevet procedure, som sikrer dette.

Resultat 2020:

24. Tilsyn med databehandlere

Kriteriet afspejler det forhold, at kommunen skal gennemføre tilsyn med sine databehandleres opfyldelse af databehandleraftalens betingelser samt implementering og opretholdelse af passende foranstaltninger for beskyttelse af persondata. Tilsyn skal gennemføres på baggrund af en risikobaseret tilgang. Der er målt på, om kommunen gennemfører tilsyn med sine databehandlere (målt procentvist).

Resultat 2020:

25. Risikovurderinger efter GDPR

Kriteriet afspejler det forhold, at kommunen skal gennemføre risikovurderinger med fokus på persondatabeskyttelse for de borgere (og

[11] Modenhedsniveau 1 = under 25%, niveau 2 = mindst 25%, niveau 3 = mindst 50%, niveau 4 = mindst 75% og niveau 5 = 100%

andre personer), som kommunen behandler oplysninger om. Det følger af ansvarlighedsprincippet, at kommunen skal kunne påvise, at der er gennemført risikovurderinger, som lever op til kravene efter GDPR. Der er målt på, om kommunen gennemfører dokumenterede risikovurderinger i overensstemmelse med GDPR.

Resultat 2020:

26. Implementering af sikkerhedsforanstaltninger

Kriteriet afspejler det forhold, at kommunen – på baggrund af risikovurderinger efter GDPR - skal implementere passende sikkerhedsforanstaltninger (tekniske og organisatoriske) for at sikre et passende sikkerhedsniveau for borgere (og andre personer), som kommunen og kommunens databehandlere behandler persondata om. Der er målt på, om kommunen har implementeret passende sikkerhedsforanstaltninger på baggrund af risikovurderinger efter GDPR.

Resultat 2020:

27. Konsekvensanalyse vedrørende databeskyttelse og tærskelvurdering

Kriteriet afspejler det forhold, at kommunen skal gennemføre en konsekvensanalyse vedrørende databeskyttelse forud for behandling af persondata, hvis det er sandsynligt, at behandlingen vil indebære en høj risiko for brud på rettigheder og frihedsrettigheder for borgere (og andre personer), der skal behandles persondata om. En konsekvensanalyse vedrørende databeskyttelse skal nedbringe uacceptabel høj risiko for rettigheder og frihedsrettigheder for de borgere (og andre personer), der skal behandles persondata om, forud for behandling. Det er nødvendigt at foretage en tærskelvurdering af en planlagt persondatabehandlings karakter, formål, sammenhæng og omfang for at identificere, om det er sandsynligt, at den pågældende planlagte behandling vil indebære en høj risiko for brud på rettigheder og frihedsrettigheder for borgere (og andre personer), der skal behandles persondata om. Der er målt på, om der foreligger en nedskrevet procedure for tærskelvurdering, som sikrer, at kommunen kan identificere, om planlagte nye behandlinger af persondata i kommunen er underlagt krav om gennemførelse af en konsekvensanalyse.

Resultat 2020:

28. Sikkerhedstest

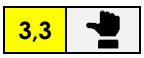
Kriteriet sikkerhedstest afspejler det forhold, at kommunen skal gennemføre sikkerhedstest, som sikrer løbende afprøvning og vurdering af implementerede sikkerhedsforanstaltningers effektivitet. Der er målt på, om der er etableret en nedskrevet procedure, som sikrer, at kommunen løbende afprøver og vurderer de implementerede foranstaltningers effektivitet.

Resultat 2020:

29. Adgangsstyring til persondata

Kriteriet afspejler det forhold, at der kun må være adgang til persondata og systemer (indeholde persondata) for kommunens medarbejdere og ledere, som er nødvendige for udførelse af deres arbejdsopgaver. Der er målt på, om der i kommunens enheder/fagområder er en nedskrevet procedure for autorisation og tildeling af rettigheder, som sikrer adgangsstyring til persondata og systemer indeholdende persondata.

Resultat 2020:



(her gennemsnit af fagområdernes/enhedernes besvarelser).

30. Inddragelse af DPO'en

Kriteriet afspejler det forhold, at kommunen skal inddrage DPO'en rettidigt og i tilstrækkeligt omfang i forhold til alle spørgsmål vedrørende beskyttelse af persondata i kommunen. Der er målt på, om der er etableret en nedskrevet procedure i kommunen, som sikrer, at kommunen kan inddrage DPO'en

rettidigt i alle spørgsmål vedrørende beskyttelse af persondata.

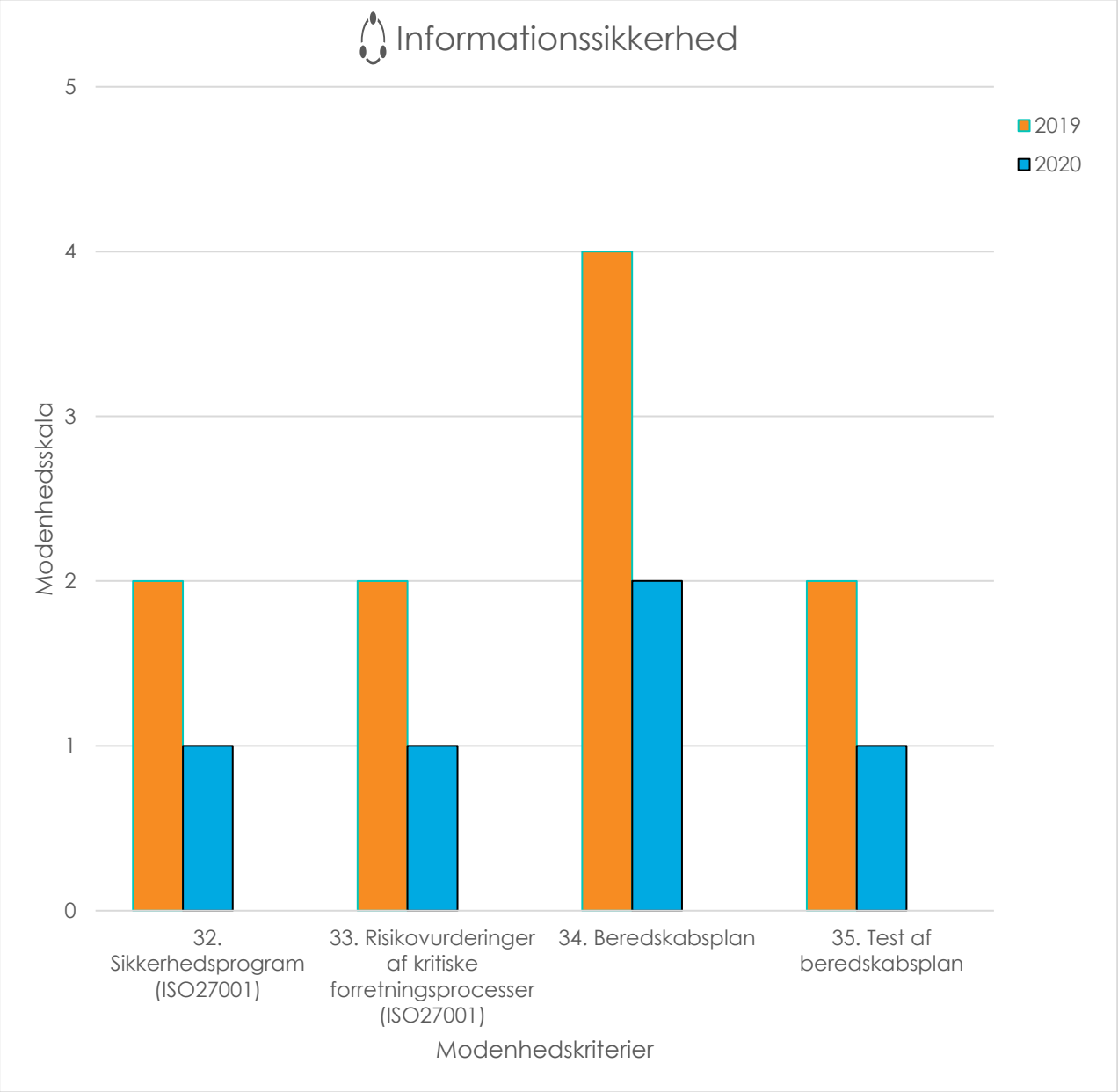
Resultat 2020:

31. Privacy by design og privacy by default

Kriteriet afspejler det forhold, at nye it-systemer/løsninger i kommunen til behandling af persondata skal være designet således, at behandlingsprincipperne efter GDPR overholdes, og persondata beskyttes (privacy by design). Eksisterende systemer/løsninger i kommunen skal konfigureres/indstilles således, at behandlingsprincipperne overholdes og persondata beskyttes (privacy by default). Der er målt på, om der er en dokumenteret implementering af principper for privacy by design og privacy by default, som sikrer, at der kan tages højde for principperne i forbindelse med implementering af nye systemer og løsninger i kommunen eller ved ændringer af eksisterende systemer.

Resultat 2020:

Informationssikkerhed



Introduktion til informationssikkerhed

Det følger af den fællesoffentlige digitaliseringsstrategi for 2016-2020, at kommunerne skal følge principperne i ISO27001. ISO27001 er en international standard for informationssikkerhed, som har til formål at bevare fortrolighed, integritet og tilgængelighed af informationsaktiver i en organisation. GDPR-modenhedsmålingen omfatter enkelte kriterier om informationssikkerhed, som udover at bevare informationsaktiver også har betydning for beskyttelse af persondata. Kriterierne afspejler ikke direkte krav efter GDPR.

32. Sikkerhedsprogram (ISO27001)

Kriteriet afspejler det forhold, at implementering og drift af informationssikkerhed i en organisation forudsætter etablering af et sikkerhedsprogram (ISO27001). Der er målt på, om et sikkerhedsprogram baseret på principperne efter ISO27001 er implementeret i kommunen.

Resultat 2020:

1

33. Risikovurderinger af kritiske forretningsprocesser

Kriteriet afspejler et princip efter ISO27001, hvorefter der skal gennemføres risikovurderinger af kritiske forretningsprocesser (og implementeres sikkerhedsforanstaltninger) for at bevare fortrolighed, integritet og tilgængelighed af informationsaktiver i organisationen. Der er målt på, om der gennemføres risikovurderinger af kritiske forretningsprocesser i kommunen.

Resultat 2020:

34. Beredskabsplan

Kriteriet afspejler et princip efter ISO27001, hvorefter der skal være en plan og en procedure (beredskabsplan) i kommunen for videreførelse af kritiske forretningsprocesser i tilfælde af kritiske situationer (fx ved et omfattende hackerangreb). Der er mål på, om der er en beredskabsplan i kommunen.

Resultat 2020:

35. Test af beredskabsplan

Kriteriet afspejler et princip efter ISO27001, hvorefter der skal være en procedure i organisationen for afprøvning og forbedring af en beredskabsplan gennem regelmæssig træning, afprøvning og evaluering, hvormed der sikres et effektivt beredskab. Uden test af beredskabsplan kan kommunen ikke vide, om en beredskabsplan virker efter hensigten i tilfælde af kritiske situationer. Der er målt på, om der er en dokumenteret procedure for test af beredskabsplan i kommunen.

Resultat 2020:

Bilag 2

Kommunens GDPR-nøgletal for 2020

DPO'en har indsamlet kommunens GDPR-nøgletal for 2020 (kommunens egne oplyste tal for performance i forhold til udvalgte GDPR-områder). I tabellerne medtages kommunens nøgletal for 2018/19.

Henvendelser fra borgere, som gør brug af rettigheder efter GDPR

Antal	2018/19	**2020**
Indsigt i egne persondata	9	7
Begrænsning af behandling af egne persondata	25	0
Berigtigelse af egne persondata	2	1
Sletning af egne persondata	3	2
Dataportabilitet	0	0
Indsigelse mod behandling af egne persondata	1	1
Indsigelse mod automatiseret afgørelse, herunder profilering	-	0
Anmodninger behandlet inden for lovfristen på 30 dage	38	10
Anmodninger besvaret inden for forlænget frist (maksimalt 3 måneder)	-	0

Kommunen har modtaget 11 henvendelser fra borgere, som har gjort brug af deres rettigheder efter GDPR. Det er et markant fald sammenlignet med 2018/19, hvor kommunen modtog 40 henvendelser.

Kommunens nøgletal viser, at kommunen har behandlet 10 ud af 11 henvendelser inden for 30-dages fristen efter tidspunktet for modtagelsen af anmodningen. Kommunen har dermed håndteret stort set alle henvendelser inden for fristen efter GDPR.

Brud på persondatasikkerheden

Antal	2018/19	**2020**
Registrerede brud på persondatasikkerheden	32	43
Brud anmeldt til Datatilsynet	22	29
Brud hvoraf der er sket underretning til borgere (eller andre personer), som er genstand for bruddet	16	14
Anmeldelser til Datatilsynet inden for lovfristen på 72 timer	20	29

Kommunen har registreret 43 brud på persondatasikkerheden. Det er en stigning sammenlignet med 2018/19, hvor kommunen registrerede 32 brud på persondatasikkerheden. Kommunen har foretaget anmeldelse til Datatilsynet i 29 brud ud af de i alt 43 brud samt underrettet borgere (eller andre personer), som er genstand for bruddet, i 14 ud af de 29 brud, som er anmeldt til Datatilsynet.

Kommunens nøgletal for 2020 viser endelig, at kommunen er blevet bedre til at anmelde brud til Datatilsynet inden for lovfristen (29 ud af 29 brud) sammenlignet med 2018/19 (20 ud af 22 brud).

Nye it-løsninger og inddragelse af DPO'en

Antal	2018/19	**2020**
Anskaffelse af nye it-løsninger til brug for behandling af persondata	3	6
Inddragelse af DPO'en ved anskaffelse af nye it-løsninger til brug for behandling af persondata	0	1

Kommunen har anskaffet 6 nye it-løsninger til brug for behandling af persondata, hvoraf DPO'en er blevet inddraget i 1 tilfælde. Kommunens inddragelse af DPO'en ved

anskaffelse af nye it-løsninger er utilstrækkelig. DPO'en skal inddrages i alle spørgsmål vedrørende beskyttelse af persondata, og det betyder, at kommunen bør inddrage DPO'en ved enhver anskaffelse af it-løsninger til brug for behandling af persondata.

Risikostyring – antal risikovurderinger, tærskelvurderinger og konsekvensanalyser

Antal	2018/19	**2020**
Gennemførte risikovurderinger	-	1
Gennemførte tærskelvurderinger	-	0
Gennemførte konsekvensanalyser	0	0
Rådføring med DPO'en ved gennemførelse af konsekvensanalyser	0	0

Kommunen har gennemført 1 risikovurdering i forhold til behandling af persondata. Kommunen har hverken gennemført tærskelvurderinger eller konsekvensanalyser vedrørende databeskyttelse.

Det er utilstrækkeligt kun at gennemføre 1 risikovurdering, når der henses til det store omfang af persondata og karakteren af persondata (følsomme og fortrolige data) i kommunen, herunder antal anskaffelser af nye it-løsninger til brug for behandling af persondata i kommunen. Risikostyring er en central komponent i en risikobaseret tilgang til GDPR, som forudsætter løbende risikovurderinger i forhold til persondatabehandling og implementering af passende sikkerhedsforanstaltninger, hvis risiciene for persondata er for høj. Uden risikovurderinger er det ikke muligt at vurdere, om der er en passende beskyttelse for persondata. Beskyttelse af persondata og privatliv er en forudsætning for tillid til digitalisering i kommunen, og beskyttelsen skal derfor gå hånd i hånd med den øgede digitalisering, som allerede er i gang i kommunen, og de nye muligheder for yderligere digitalisering og brug af data.

Det forekommer desuden utilstrækkeligt, at kommunen ikke har gennemført tærskelvurderinger, da kommunen uden tærskelvurderinger ikke kan identificere, om kommunen i forhold til planlagte nye behandlinger af persondata er omfattet af krav om gennemførelse af konsekvensanalyse vedrørende databeskyttelse forinden behandling af persondata. God risikostyring forudsætter løbende gennemførelse af tærskelvurderinger i forhold til planlagte nye behandlinger af persondata i kommunen samt hvis påkrævet gennemførelse af konsekvensanalyser vedrørende databeskyttelse.

DPO'en har i 2020 gennemført et webinar om risikovurderinger, tærskelvurderinger og konsekvensanalyser vedrørende databeskyttelse og udarbejdet skabeloner til arbejdet med risikovurderinger og tærskelvurderinger, som kommunen kan anvende til den store opgave med risikostyring.

Tilsyn/henvendelser/påtaler og bøder fra Datatilsynet

Antal	2018/19	**2020**
Tilsyn	0	1
Emner for tilsyn:	-	Behandling af persondata i Ishøj Svømmehal
Øvrige skriftlige henvendelser/forespørgsler fra Datatilsynet/anmodning fra Datatilsynet om uddybning af spørgsmål vedrørende brud på persondatasikkerheden	-	2
Påtaler/påbud/kritik fra Datatilsynet	-	0
Bøder fra Datatilsynet	0	0

Datatilsynet har iværksat 1 tilsyn af kommunen vedrørende behandling af persondata i Ishøj Svømmehal på baggrund af en klage fra en bruger af svømmehallen. Tilsynssagen vedrørende behandling af persondata i

Ishøj Svømmehal er verserende hos Datatilsynet.

Datatilsynet har i 2 tilfælde fulgt op over for kommunen og bedt om en uddybning vedrørende brud på persondatasikkerheden i Ishøj Kommune, hvorefter Datatilsynet har lukket opfølgningssagerne.

Interne kontroller i kommunen med overholdelse af GDPR

Antal	2018/19	**2020**
Planlagte tilsyn	1	0
Emne for planlagt tilsyn	(skriftlige fortegnelser over behandlinger af persondata i fagområder)	-
Gennemførte tilsyn	1	0
Emne for gennemført tilsyn	(se ovenfor)	-

Kommunen har ikke interne kontroller med overholdelse af GDPR i kommunen. Det er en tilbagegang sammenlignet med 2018/19, hvor kommunen gennemførte 1 kontrol. Det er utilstrækkeligt, at kommunen ikke har gennemført interne kontroller i 2020. Det følger af GDPR, at kommunen løbende skal tjekke overholdelsen af GDPR med interne kontroller for at sikre kommunens GDPR-compliance.

Kommunens GDPR-ressourcer

Antal	2018/19	**2020**
Dedikerede årsværk til implementering og drift af GDPR[12]	1	1 [13]
Øvrige årsværk til implementering og drift af GDPR[14]	0	0,5

Kommunen har i alt 1,5 årsværk til GDPR. Antal årsværk til GDPR i 2020 er opnormeret med 0,5 sammenlignet med 2018/19, hvilket er positivt. Kommunen bør dog overveje, om ressourcerne er tilstrækkelige til at udvikle en risikobaseret tilgang til GDPR (se afsnittet ovenfor om risikostyring).

Opsamling

Der har været et fald i antal henvendelser fra personer, som har gjort brug af deres rettigheder efter GDPR i 2020. Kommunen har håndteret stort set alle henvendelser inden for lovfristen på 30 dage efter tidspunktet for modtagelsen af anmodningen.

Der har været en stigning i antal registrerede brud på persondatasikkerheden i 2020. Men kommunen er blevet bedre til at anmelde brud til Datatilsynet inden for lovfristen på 72 timer.

Kommunen inddrager ikke DPO'en tilstrækkeligt ved anskaffelse af nye it-løsninger til brug for behandling af persondata.

Kommunen har gennemført 1 risikovurdering i 2020, men hverken gennemført tærskelvurderinger eller konsekvensanalyser vedrørende databeskyttelse. Det er utilstrækkeligt kun at gennemføre 1 risikovurdering. Uden løbende risikovurderinger kan kommunen ikke vurdere, om der er en passende beskyttelse af persondata i kommunen. Det forekommer desuden utilstrækkeligt, at kommunen ikke har gennemført tærskelvurderinger. Uden tærskelvurderinger kan kommunen ikke identificere, om planlagte nye behandlinger af persondata er underlagt krav om gennemførelse af konsekvensanalyse vedrørende databeskyttelse forinden behandling af persondata.

I 2020 har Datatilsynet iværksat 1 tilsyn af kommunen vedrørende behandling af persondata i Ishøj Svømmehal. Tilsynssagen vedrørende behandling af persondata i

[12] Medarbejdere i kommunen, som udelukkende beskæftiger sig med GDPR.

[13] Pr. 15. august 2020.

[14] Medarbejdere i kommunen, som delvist beskæftiger sig med GDPR.

Ishøj Svømmehal er verserende hos Datatilsynet.

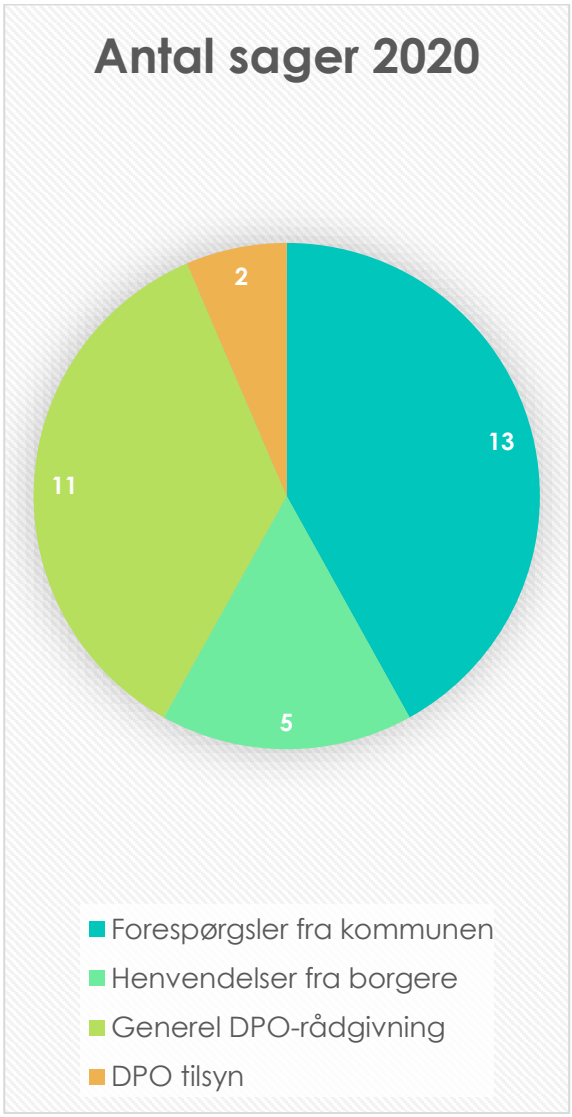
Datatilsynet har i 2 tilfælde fulgt op over for kommunen med spørgsmål vedrørende brud på persondatasikkerheden i Ishøj Kommune, hvorefter tilsynet har lukket de pågældende opfølgningssager.

Kommunen har ikke gennemført interne kontroller med overholdelse af GDPR i kommunen i 2020, hvilket er utilstrækkeligt. Kommunen skal gennemføre interne kontroller for at sikre kommunens GDPR-compliance.

Kommunen har i alt 1,5 årsværk til GDPR. Kommunen bør overveje, om ressourcerne er tilstrækkelige til at udvikle en risikobaseret tilgang til GDPR, som forudsætter løbende gennemførelse af risikovurderinger, tærskelvurderinger samt hvis påkrævet gennemførelse af konsekvensanalyser vedrørende databeskyttelse.

Bilag 3

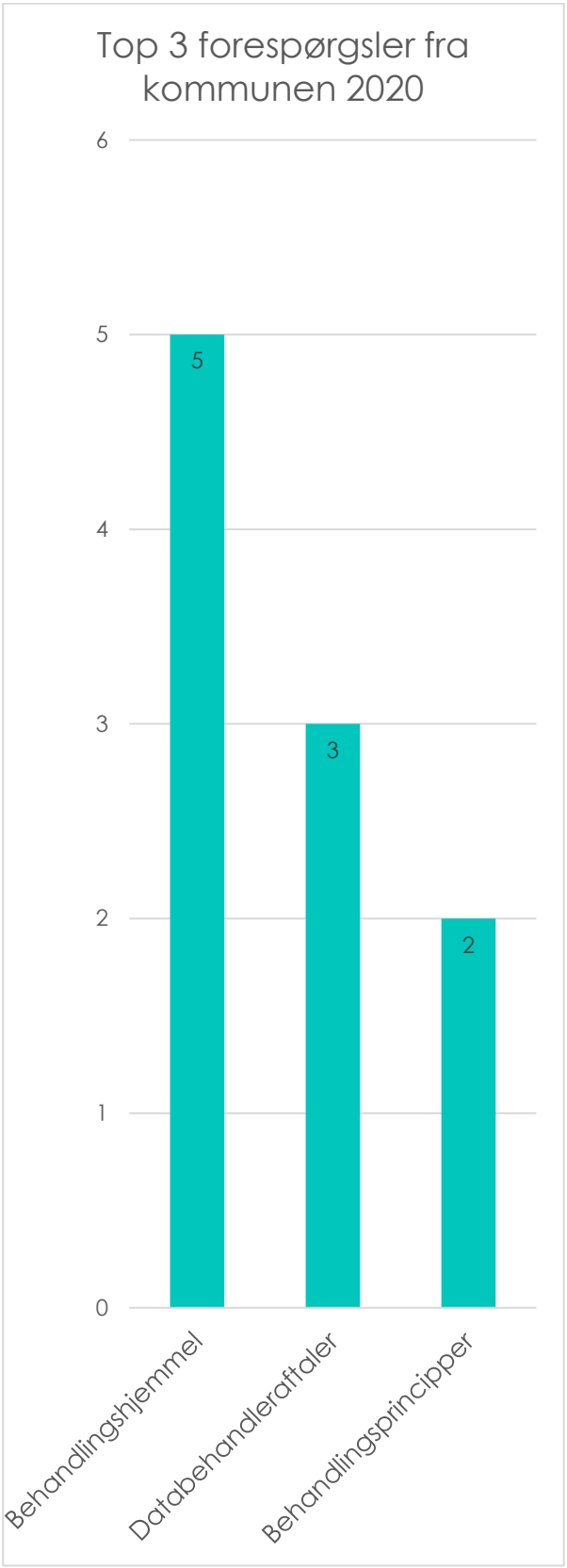
Sagsstatistik for DPO'ens arbejde



Antal sager

DPO'en har i perioden 1. januar 2020 til og med 31. december 2020 oprettet i alt 31 sager, som er fordelt på sagskategorierne: forespørgsler fra kommunen (13 sager), henvendelser fra borgere (5 sager), generel DPO-rådgivning (11 sager) samt DPO-tilsyn, som omfatter DPO'ens tilsyn med kommunen samt et tilsyn med kommunens Børn- og Ungeudvalg (i alt 2 tilsyn).

Hyppigste forespørgsler fra kommunen

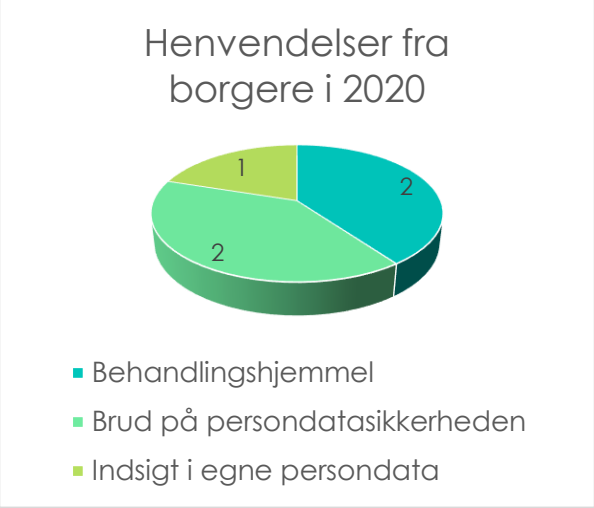


Den hyppigste forespørgsel handler om behandlingshjemmel, hvor DPO'en har modtaget 5 forespørgsler fra kommunen om bl.a. hjemmel til behandling af billeder, indhentelse af samtykke samt hjemmel til persondatabehandling hos TV-Ishøj.

Næsthyppigste forespørgsel handler om databehandleraftaler og spørgsmål om databehandlerkonstruktion, hvor DPO'en har modtaget 3 forespørgsler om bl.a. brug af underdatabehandlere.

Herefter kommer forespørgsler om behandlingsprincipper efter GDPR, hvor DPO'en har modtaget 2 forespørgsler om hhv. opbevaringsfrister for persondata hhv. overholdelse af behandlingsprincipper i forbindelse med videoovervågning i kommunen.

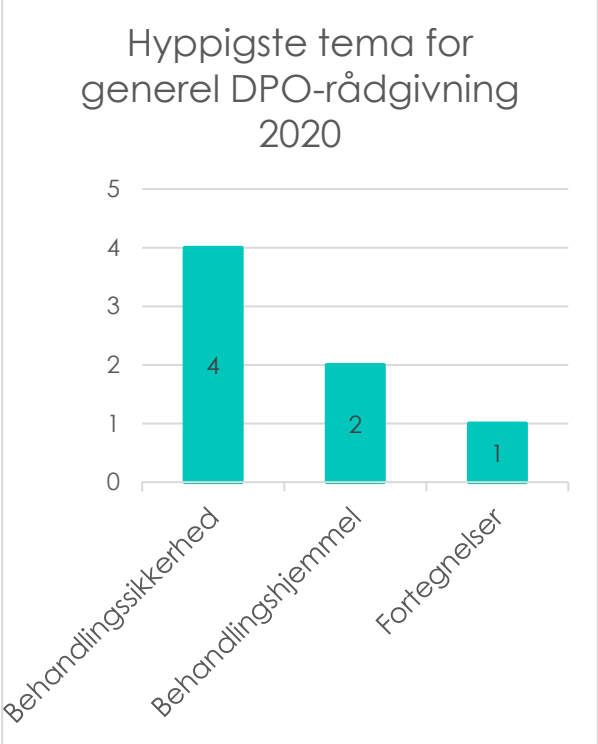
Henvendelser fra borgere



DPO'en har modtaget i 5 henvendelser fra borgere i 2020. 2 henvendelser omhandler spørgsmål om behandlingshjemmel til behandling af persondata i Ishøj Svømmehal. 2 henvendelser omhandler brud på persondatasikkerheden i kommunen. 1 henvendelse omhandler anmodning om indsigt i egne persondata hos Ishøj Svømmehal. DPO'en har vejledt borgerne og videreformidlet henvendelserne til foranstaltning i Ishøj Kommune.

Generel DPO-rådgivning

Sagskategorien generel DPO-rådgivning omfatter sager, hvor DPO'en af egen drift rådgiver, giver anbefalinger eller holder oplæg for kommunerne i Den Storkøbenhavnske Digitaliseringsforening, som er omfattet af DPO-funktionen[15].



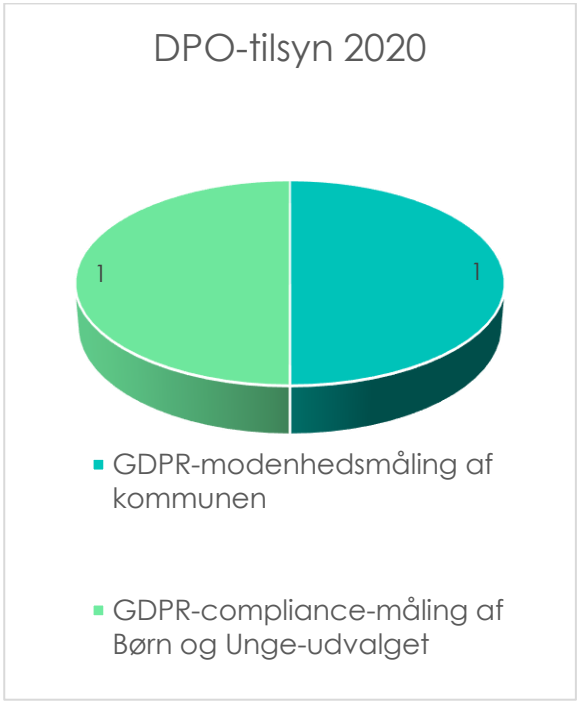
Det hyppigste tema for generel DPO-rådgivning vedrører behandlingssikkerhed, hvor DPO'en dels har gennemført et webinar for kommunerne i Den Storkøbenhavnske Digitaliseringsforening om risikovurderinger og konsekvensanalyser/tærskelvurderinger og dels har DPO'en gennemført et oplæg om konsekvensanalyse vedrørende databeskyttelse i forhold til behandling af persondata i Aula samt rådgivet og udsendt anbefalinger om beskyttelse af persondata under hjemmearbejde i forbindelse med COVID-19-restriktioner.

[15] DPO-funktionen i Den Storkøbenhavnske Digitaliseringsforening omfatter 9 ud af 11 medlemskommuner i Den Storkøbenhavnske Digitaliseringsforening. DPO-funktionen består af 2 DPO'er. Den ene er DPO for Rødovre, Glostrup, Ishøj, Herlev og Solrød Kommune, og den anden er DPO for Hvidovre, Dragør, Høje Taastrup og Albertslund Kommune.

Det næsthyppigste tema handler om behandlingshjemmel, hvor DPO'en i to sager har rådgivet og givet anbefalinger til kommunerne i Den Storkøbenhavnske Digitaliseringsforening vedrørende spørgsmål om lovlig overførsel af persondata til tredjelande i anledning af ny retspraksis fra EU-Domstolen (Schrems II-dommen).

DPO'en har i en sag (tredjehyppigste tema) rådgivet og givet anbefalinger til kommunerne i Den Storkøbenhavnske Digitaliseringsforening vedrørende opdatering af kommunernes fortegnelser over behandlingsaktiviteter i anledning af en opdateret vejledning fra Datatilsynet om samme.

DPO-tilsyn



DPO'en har udført et enkelt tilsyn med kommunens overholdelse af GDPR ved gennemførelse af en GDPR-modenhedsmåling i november 2020 (se bilag 1).

DPO'en har desuden i 2. kvartal 2020 ført et tilsyn med overholdelse af GDPR i kommunens Børn- og Ungeudvalg, som DPO'en af kommunen er udpeget som rådgiver for som en del af kommunens sekretariatsbistand til enheden. Børn- og Ungeudvalget har karakter af offentligt organ, som er selvstændig dataansvarlig efter GDPR, og som derfor skal have en DPO, og selv er ansvarlige for at overholde reglerne i GDPR.

DPO'en har udført tilsynet med overholdelse af GDPR i Børn- og Ungeudvalget i kommunen ved gennemførelse af en måling, som er besvaret af en udpeget respondent for enheden (selvevaluering). Resultaterne for målingen af Børn- og Ungeudvalget viser generelt, at der i forhold til flere forhold er plads til forbedring af GDPR-compliance i enheden.

Møder i 2020

DPO'ens mødeaktivitet har været stærkt begrænset i 2020 grundet COVID-19-restriktioner. DPO'en har i stedet deltaget i ad hoc-møder, bl.a. om modenhedsmålinger samt deltaget regelmæssigt i onlinemøder (såkaldte GDPR-fortolkningsmøder) for sikkerhedskoordinatorerne fra kommunerne i Den Storkøbenhavnske Digitaliseringsforening.

Leverancer

DPO'en har udviklet et skræddersyet undervisningsforløb til kommunerne i Den Storkøbenhavnske Digitaliseringsforening i 2020 samt udarbejdet vejledninger og skabeloner med henblik på at understøtte kommunerne i forhold til GDPR-compliance.

Opsamling

Antallet af sager, hvor kommunen har henvendt sig til DPO'en i 2020, viser, at kommunen har gjort brug af DPO'en. Henvendelserne fra kommunen spænder over mange forskellige databeskyttelsesretlige spørgsmål, men de hyppigste henvendelser handler om behandlingshjemmel, databehandleraftaler og behandlingsprincipper efter GDPR. DPO'en har modtaget 5 henvendelser fra borgere i 2020. Henvendelser omhandler spørgsmål om behandlingshjemmel til behandling af persondata i Ishøj Svømmehal, brud på persondatasikkerheden i kommunen samt indsigt i egne persondata i Ishøj Svømmehal. Sagerne, hvor DPO'en af egen drift rådgiver og giver anbefalinger til kommunerne i Den Storkøbenhavnske Digitaliseringsforening, har fortrinsvis omhandlet spørgsmål om behandlingssikkerhed og behandlingshjemmel.

DPO'en har i 2020 udført et tilsyn med kommunens overholdelse af GDPR ved gennemførelse af den årlige GDPR-modenhedsmåling. Derudover har DPO'en gennemført et tilsyn med overholdelse af GDPR i Børn- og Ungeudvalget.

DPO'ens fysiske mødeaktivitet i kommunen har været stærkt begrænset grundet COVID-19-restriktioner, men DPO'en har i stedet deltaget i ad hoc-onlinemøder med kommunen samt deltaget i regelmæssige møder med sikkerhedskoordinatorerne fra kommunerne i Den Storkøbenhavnske Digitaliseringsforening (GDPR-fortolkningsmøder).

DPO'en har i 2020 udviklet et skræddersyet undervisningsforløb til kommunerne i Den Storkøbenhavnske Digitaliseringsforening samt udarbejdet vejledninger og skabeloner med henblik på at understøtte kommunerne i forhold til at opnå GDPR-compliance.