DATABESKYTTELSESRÅDGIVERENS ÅRSRAPPORT 2022

Afsender:

,

DPO-funktionen i Den Storkøbenhavnske Digitaliseringsforening

Modtager:

Kommunalbestyrelsen i Rødovre Kommune

Indhold

Indledning

I 2022 har DPO-funktionen i DSD skiftet en medarbejder ud. DPO Christian Abildløkke Rasmussen tiltrådte i foråret 2022, for Albertslund, Dragør, Hvidovre og Høje Taastrup kommuner. Derudover så 2022 en forandring i DPO-funktionens omfang, da Vallensbæk kommune valgte at underskrive tjenesteydelsesaftalen med DSD og derved indgik som en del af DPO-funktionens ansvarsområde med Andreas Drægert som DPO. Der er nu 10 kommuner i Den Storkøbenhavnske Digitaliseringsforening der modtager DPO service via tjenesteydelsesaftale.
DPO-funktionen har varetaget service med at rådgive og vejlede kommunerne samt foretage tilsyn med om kommunerne også overholder bestemmelserne i lovgivningen.
I 2022 har DPO-funktionen således ført tilsyn med kommunernes overholdelse af tilsynsforpligtelsen overfor databehandlere og leveret en tilsynsrapport. DPO-funktionen har foretaget modenhedsmåling på en udvalgt mængde af kommunernes selvejende institutioner, råd, nævn og udvalg. Afslutningsvis på året, har DPO-funktionen iværksat den årlige modenhedsmåling og årets sidste tilsyn, hvor der blev bedt om redegørelse for kommunernes håndtering af databrud.
2022 blev året med nye og store afgørelser, hvor der blev truffet beslutninger i stor stil fra de nationale datatilsyn i de forskellige europæiske lande. Ikke mindst i Irland, hvor der blev truffet flere historiske afgørelser overfor Meta (moderselskab for bl.a. Facebook), med bøder i milliard-størrelsen. Men også hos det danske datatilsyn lagde man sig ud med tech-giganterne. Andet halvår af 2022 startede midt i sommerferien med at det danske datatilsyn gav påbud og forbud til Helsingør kommune om at indstille driften af deres system til at drive undervisning i kommunens skoler. Pga. mangelfuld dokumentation og redegørelse for brug af systemet Google Workspace for Education, kunne Datatilsynet ikke acceptere kommunens fortsatte brug og forbød brugen øjeblikkeligt, med et dertil hørende påbud om at sørge for at systemet blev gjort lovligt at bruge eller skille sig af med det. Dette skabte ringe i vandet, der stadig breder sig. Påbuddet om lovliggørelse blev gjort til et fælles projekt for alle kommuner der benytter sig af systemet til skolebrug og er stadig en sag der afventer endelig afgørelse i 2023. Først her i begyndelsen af 2023 er det endelige vurderingsmateriale afleveret til Datatilsynet. Der afventes en afgørelse inden 1. halvårs slut.
Internationalt er der sket store ting i 2022. Den amerikanske præsident Joe Biden og præsidenten for EU-kommissionen Ursula von der Leyen meldte offentligt ud i marts 2022, at man principielt ville mødes om en aftale, der skulle sikre at overførsler af data mellem EU og USA ikke længere var ulovlige. Forventningen er, at selvom der bliver stemt for en vedtagelse af aftalen, står privatlivsaktivisterne i kø for at starte næste sag op hos den Europæiske Domstol.
Kommunerne i Den Storkøbenhavnske Digitaliseringsforening er, som alle andre, underlagt de spilleregler og den usikkerhed der har været for brug af amerikanske selskaber og cloud-leverandører i almindelighed siden Schrems II dommen, hvor USA blev kategoriseret som et usikkert tredjeland, med lovgivning der ikke sikrer europæiske borgere en tilsvarende retspraksis som i EU.
Den usikkerhed og problematik Schrems II skabte, viser i mange henseender hvor kompliceret en opgave det er at skulle vurdere krav til privatlivsbeskyttelse, forretningspraksis, omkostninger og serviceniveau i software-løsninger og hardware-indkøb.
Det kræver dygtighed, integritet og standhaftighed at stå fast på sikring af privatlivets fred, når kravene kommer mange steder fra. Heldigvis er DPO-funktionen velsignet med en samarbejdsflade hos kommunerne, hvor dygtige fagpersoner opsøger og deler viden kommunerne imellem. I mange sammenhænge ser DPO-funktionen en stigende interesse og evne hos kommunerne i at skabe en sammenhængende efterlevelse af reglerne i databeskyttelseslovgivningen og at skabe synergier i arbejdet mellem sig.
Vi glæder os til et 2023, hvor der helt sikkert vil ske en masse spændende ting på dette område. Eksempelvis ved vi allerede, at Datatilsynet agter at føre tilsyn med rollen som DPO i 2023.

Med venlig hilsen - Christian Abildløkke Rasmussen og Andreas Drægert

Status for overholdelse af GDPR i kommunen

Resultater for GDPR-modenhedsmåling 2022

DPO-funktionen gennemførte i november 2022 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).

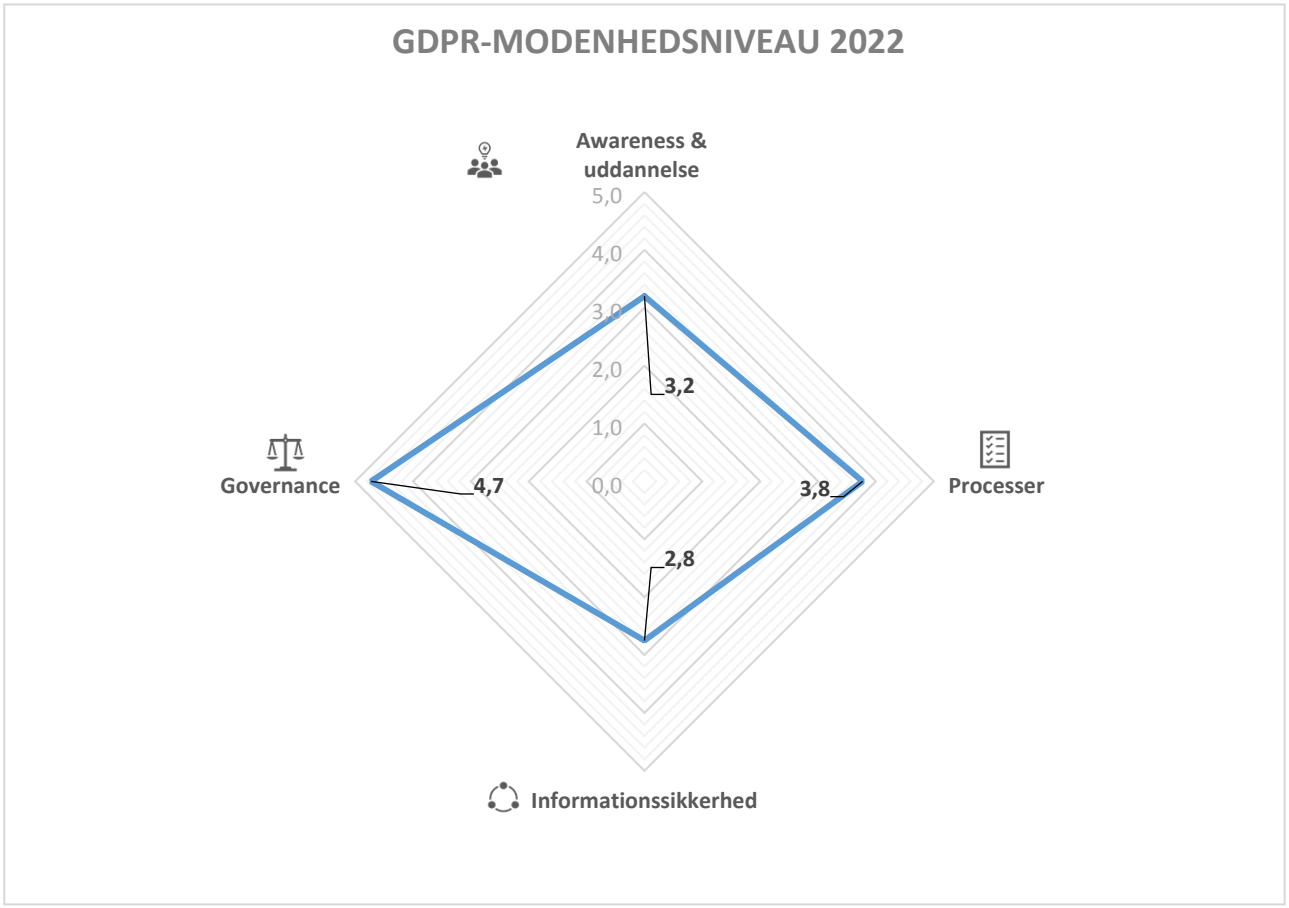
Målingen udgøres af besvarelser fra udpegede respondenter i kommunen (selvevaluering), og resultaterne udgør kommunens GDPR-modenhedsniveau for 2022.

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 kriterier om indgåelse af databehandleraftaler, gennemførelse af tilsyn med databehandlere samt gennemførsel af risikovurderinger for behandling, hvor niveau 5 svarer til 100 % overholdelse af GPDR-krav.

Model 1: Gennemsnitsresultater for 2022 fordelt på fire hovedområder[2]



DPO'ens vurdering

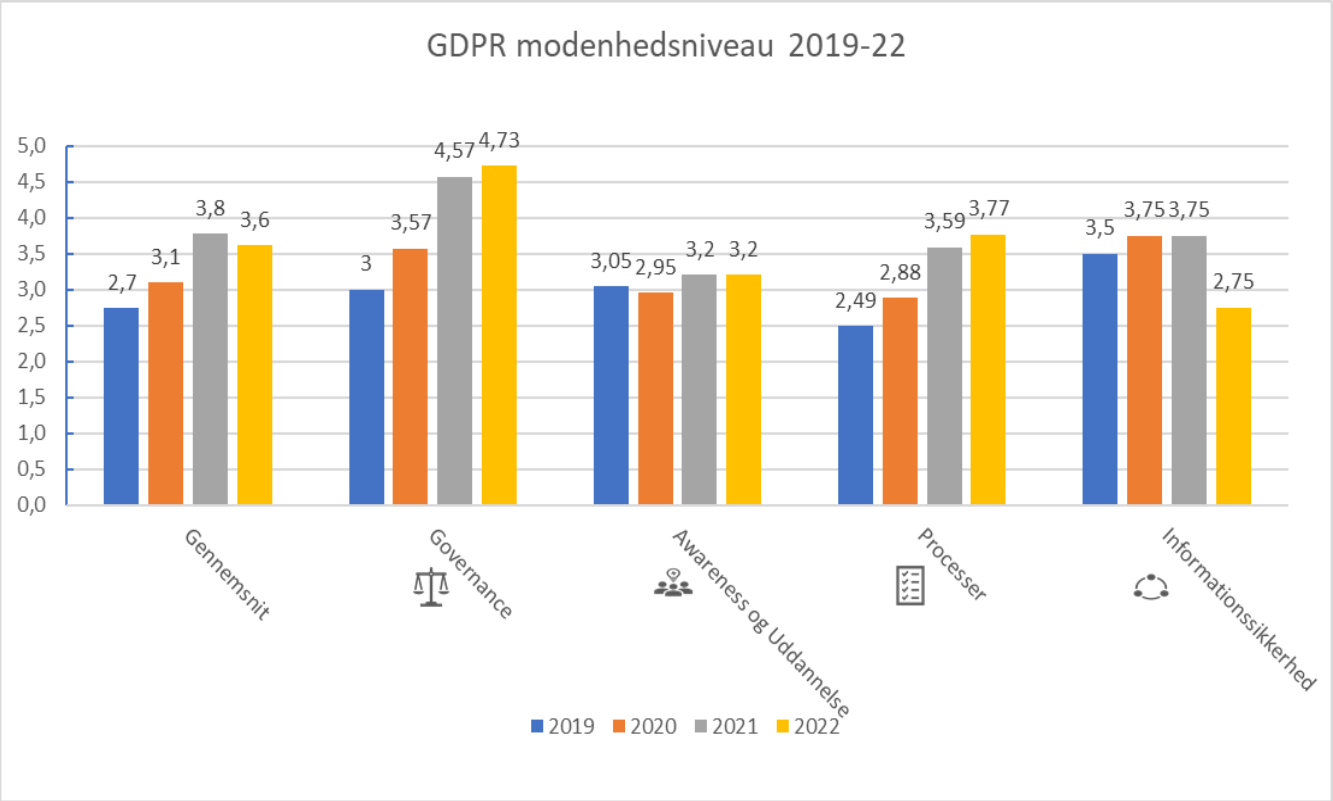
Samlet set viser resultatet for GDPR-modenhedsmålingen i 2022, at kommunens GDPR-modenhedsniveau er 3 eller højere i forhold til 3 af de overordnede 4 kriterier for opfyldelse af GDPR-krav. Det indikerer, at kommunen på tidspunktet for målingen har standardiseret efterlevelse af krav for Awareness og uddannelse samt Processer. Kriteriet Governance er opfyldt i en sådan grad, at der løbende tages stilling til at kontrollere processer og bruge dem aktivt i arbejdet med GDPR. I 2022 har kommunen scoret under 3 på kriteriet for Informationssikkerhed. Dette er fordi der er taget stilling til at score hhv. modenhed om beredskab og beredskabstest lavere end 2021.

Kommunens gennemsnitlige GDPR-modenhedsniveau i 2022 er 3,6, og modenheden er dermed faldet med 0,2 sammenlignet med målingen i 2021, hvor gennemsnitsniveauet var 3,8.

Kommunens indsats i 2022 har således udmøntet sig i et modenhedsniveau, der i gennemsnit er stort set ens med 2021 på samtlige parametre, bortset fra det specifikke udslag der vedrører kriteriet Informationssikkerhed.

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

Model 2: Resultat af GDPR-modenhedsmåling i 2022 sammenlignet med målingen i 2021, 2020 og 2019



Kommunens GDPR-nøgletal 2022

De indsamlede nøgletal som DPO-funktionen har vedlagt i Bilag 2 viser samlet set tre særlige udslag ift. 2021.

- Rødovre kommune har iværksat procedure med interne kontroller med overholdelse af GDPR og udført 4 tilsyn i løbet af 2022. Dette er en direkte opfølgning på anbefaling fra 2021. Således har Rødovre kommune udvist handlekraft og dokumenterer nu intern opfølgning på egne retningslinjer.

- Rødovre kommune har ikke kunnet bibeholde det samme antal risikovurderinger i 2022 som 2021. Det skal forstås sådan, at Rødovre kommune tidligere har udført deres risikovurderinger, men at de skal genbesøges løbende. Hvis Rødovre kommunes procedure for gennemgang af risikovurderinger tager højde for risikoen for de registreredes rettigheder og frihedsrettigheder, så kan det godt være at tallet afspejler, at kommunen har genbesøgt de vigtigste (hvor der er størst risiko for de registrerede).

- Rødovre kommune har i løbet af 2022 arbejdet med færre ressourcer end i 2021. Der er angivet en faktor på 1 årsværk, som er blevet fjernet fra arbejdet. Det er essentielt for overholdelse af lovgivningen, at der er afsat tilstrækkelige ressourcer til arbejdet med GDPR.

DPO'ens anbefaling samt forslag til kontrol

DPO'ens anbefaling på baggrund af kommunens GDPR-nøgletal 2022 og GDPR-modenhedsmåling 2022	Forslag til kontrol
• Sikkerhedstest 	Udarbejde procedure for og gennem den procedure udføre tests af de sikkerhedsforanstaltninger der eksisterer for behandlingsaktiviteter i kommunen. Dette for at sikre, at foranstaltningerne virker efter hensigten og reelt er med til at sænke risikoen for de registrerede.
• Beredskabsplan og test af beredskabsplan 	Udarbejde beredskabsplan for kommunens informationssikkerhedsaktiver og holde den opdateret. Derudover udarbejde procedure for og teste beredskabsplanen efter den procedure, for beredskabsplaner der eksisterer i kommunen.

Bilag 1 - GDPR-modenhedsmåling

Formål

GDPR-modenhedsmålingen af kommunen i november 2022 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.

I dette bilag vises de samlede resultater for GDPR-modenhedsmålingen i 2022. For sammenligningens skyld gengives resultaterne for 2020 og 2021 i samme diagram.

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.

Metode

Målingen af GDPR-modenheden er baseret på principper fra den anerkendte AICPA Privacy Maturity Model[3]. 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. I årets iteration af modenhedsmålingen er der indsat en stikprøvekontrol for begge besvarelsesområder, hvor den centrale måling har skullet uploade materiale til dokumentation, hvis der er svaret modenhedsniveau 3 eller over på skalaen. Derudover er der udvalgt enkelte områder for hver enkelt kommunes fagområdes-/enheds-besvarelse hvor der også er foretaget en stikprøvekontrol. DPO-funktionen kommenterer og justerer på kommunens selvevaluering, hvis ikke dokumentationen udleveret ved kontrollen lever op til de forudsatte kriterier.

Modenhedskriterier

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

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

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. Kendskab til politikker for beskyttelse af persondata
7. Intern kontrol med overholdelse af politikker og GDPR-compliance *
8. Årshjul for GDPR-arbejdsopgaver

Awareness og uddannelse

9. Awareness*
10. Uddannelse*

Processer

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

Informationssikkerhed

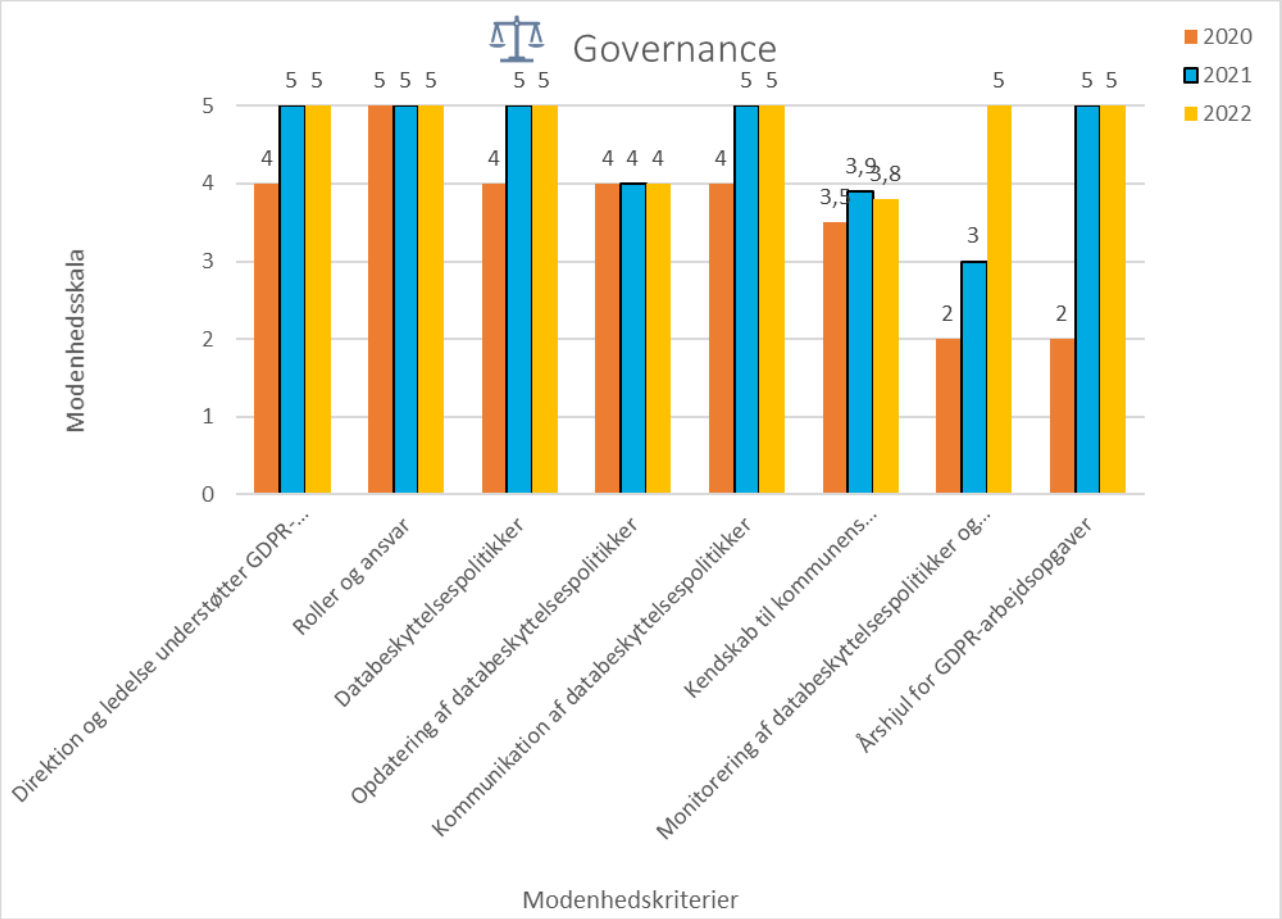
34. Sikkerhedsprogram (ISO27001)
35. Risikovurderinger af kritiske forretningsprocesser (ISO27001)
36. Beredskabsplan
37. Test af beredskabsplan

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



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.

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.

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.

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.

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.

Kommunikation 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.

Kendskab til kommunens databeskyttelsespolitikker

Kriteriet afspejler det forhold, at kommunens politikker for databeskyttelse skal være udbredt til og kendt af kommunens medarbejdere og ledere. Der er målt på, om politikker for beskyttelse af persondata er kendt af medarbejdere og ledere.

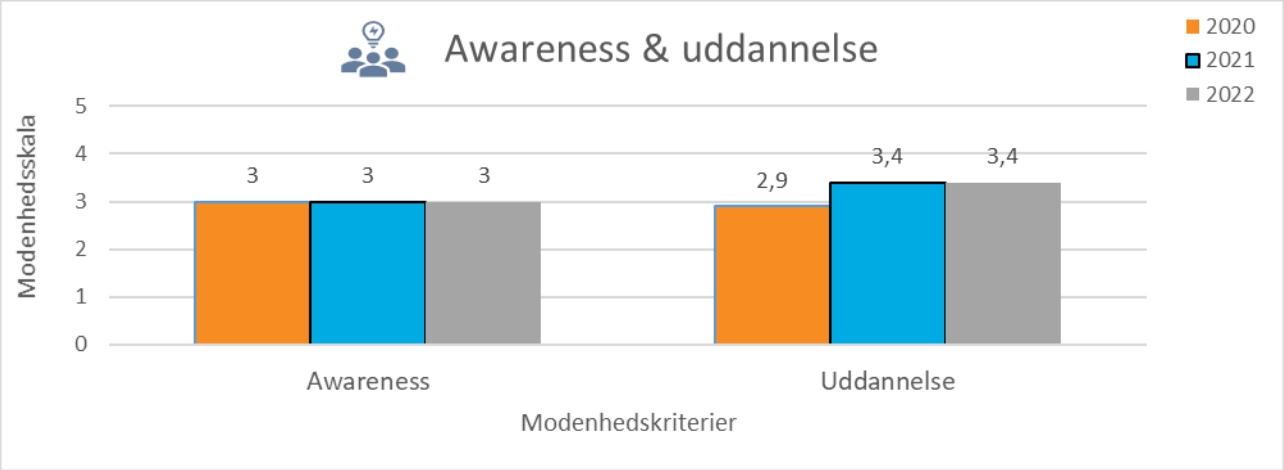
Intern kontrol med overholdelse af politikker og GDPR-compliance

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.

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).

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.

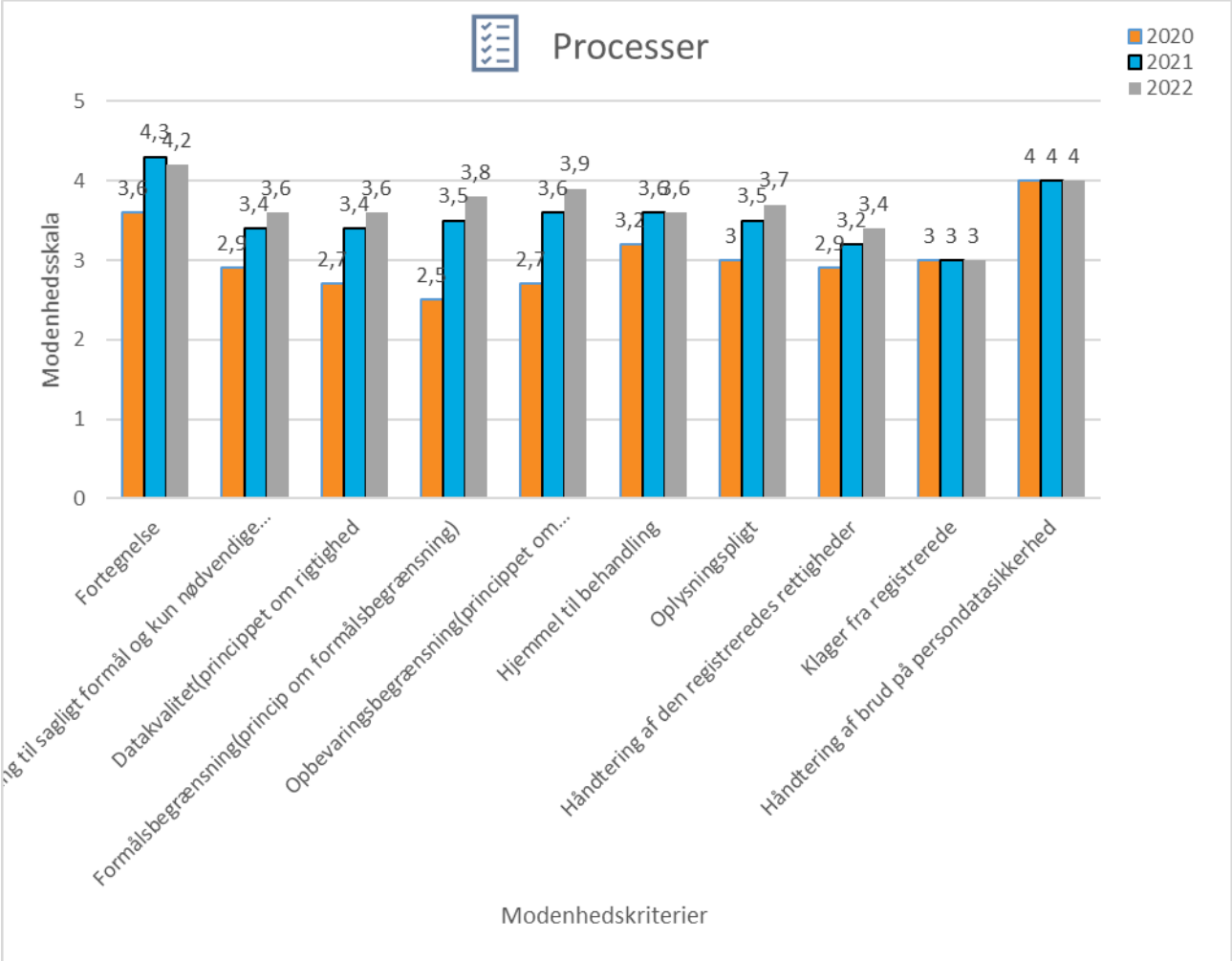
Awareness

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.

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.

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.

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.

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.

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.

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).

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.

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.

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.

Behandlingshjemmel

Kriteriet afspejler det forhold, at behandling af persondata, som sker i kommunen, skal have en gyldig lovhjemmel efter GDPR. Der er målt på, om der i enheder/fagområder er en nedskrevet procedure som sikrer, at der kun indsamles og behandles personoplysninger med en gyldig hjemmel.

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.

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

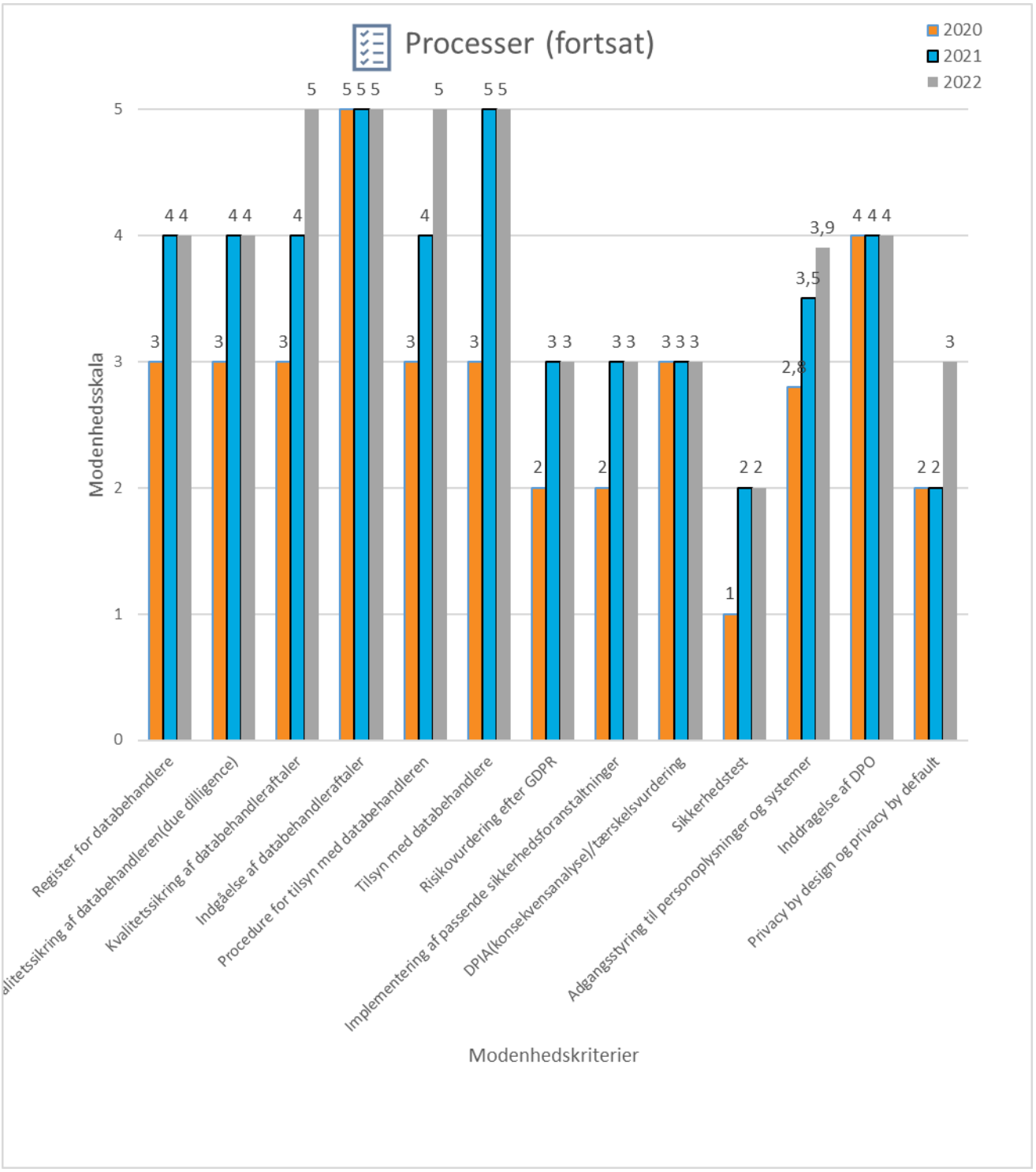
Kriteriet afspejler det forhold, at kommunen rettidigt skal håndtere henvendelser fra borgere (og andre personer), som kommunen behandler persondata, som gør brug af deres rettigheder efter GDPR (fx indsigt i egne persondata). Der er målt på, om der i kommunens enheder/fagområderne er en nedskrevet procedure,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

Klager fra den registrerede

Kriteriet afspejler det forhold, at kommunen rettidigt skal behandle klager fra borgere (og andre personer) som kommunen behandler persondata om, og som gør brug af deres ret til at klage over behandlingen. Der er målt på, om der i kommunens enheder/fagområder er en nedskrevet procedure, som sikrer håndtering af klager fra borgere.

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.



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.

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.

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.

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)4.

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.

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).

Risikovurderinger efter GDPR

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

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.

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

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.

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.

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.

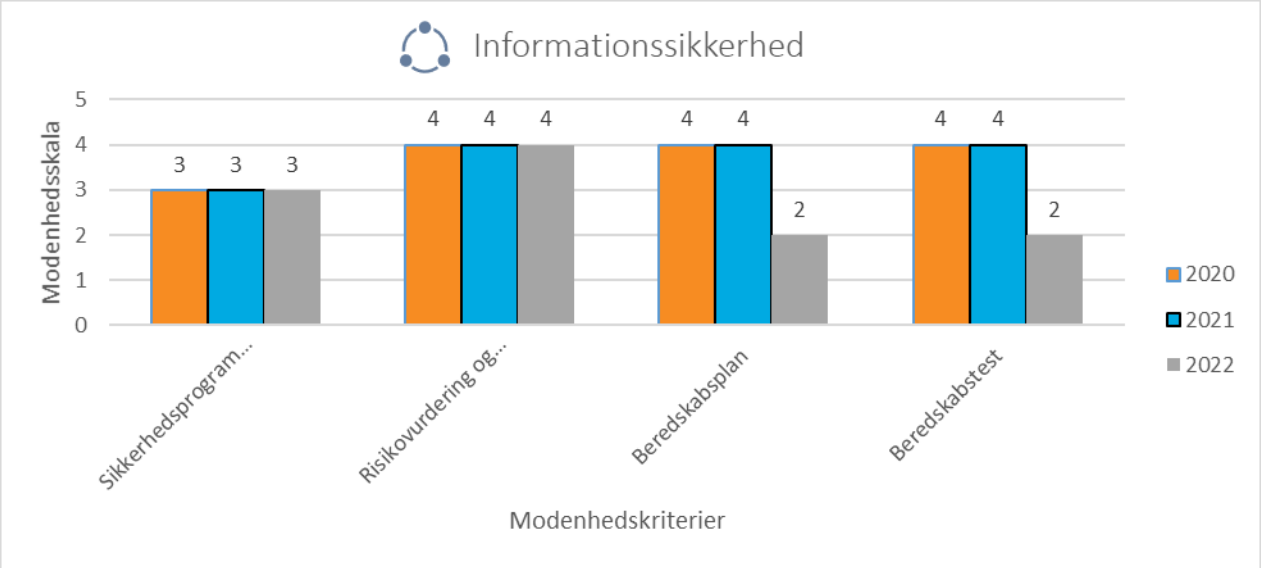
Inddragelse af DPO'en

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

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.

Informationssikkerhed



Introduktion til informationssikkerhed

Arbejdet med kommunerne informationssikkerhed skal følge principperne i ISO27001. Det blev aftalt i den fællesoffentlige digitaliseringsstrategi fra 2016-2021. Derudover arbejder staten med minimumskrav til tekniske foranstaltninger ift. informationssikkerhed, hvilket KL anbefaler kommunerne at skele til.
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.

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.

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.

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 målt på, om der er en beredskabsplan i kommunen.

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.

Bilag 2 – Nøgletal

Henvendelser fra borgere, som har gjort brug af deres rettigheder efter GDPR

Antal	2020	2021	**2022**
Indsigt i egne persondata	6	13	7
Begrænsning af behandling af egne persondata	N/A	N/A	N/A
Berigtigelse af egne persondata	N/A	N/A	N/A
Sletning af egne persondata	N/A	N/A	N/A
Dataportabilitet	N/A	N/A	N/A
Indsigelse mod behandling af egne persondata	N/A	N/A	N/A
Indsigelse mod automatiseret afgørelse, herunder profilering	N/A	N/A	N/A
Anmodninger behandlet inden for lovfristen på 30 dage	6	13	7
Anmodninger besvaret inden for forlænget frist (maksimalt 3 måneder)	0	0	0

Brud på persondatasikkerheden

Antal	2020	2021	**2022**
Registrerede brud på persondatasikkerheden	19	36	40
Brud anmeldt til Datatilsynet	12	23	22
Brud hvoraf der er sket underretning til borgere (eller andre personer), som er genstand for bruddet	12	21	15
Anmeldelser til Datatilsynet inden for lovfristen på 72 timer	11	23	21

Nye it-løsninger og inddragelse af DPO'en

Antal	2020	2021	**2022**
Anskaffelse af nye it-løsninger til brug for behandling af persondata	12	22	15
Inddragelse af DPO'en ved anskaffelse af nye it-løsninger til brug for behandling af persondata	1	7	10

Risikostyring – antal risikovurderinger efter GDPR, tærskelvurderinger og konsekvensanalyser vedrørende databeskyttelse

Antal	2020	2021	**2022**
Gennemførte risikovurderinger	3	333	174
Gennemførte tærskelvurderinger	1	1	3
Gennemførte konsekvensanalyser	1	0	0
Rådføring med DPO'en ved gennemførelse af konsekvensanalyser	1	0	0

Tilsyn/henvendelser/påtaler og bøder fra Datatilsynet

Antal	2020	2021	**2022**
Tilsyn	0	0	1
Emner for tilsyn:			Modenhedsvurdering
Øvrige skriftlige henvendelser/forespørgsler fra Datatilsynet/anmodning fra Datatilsynet om uddybning af spørgsmål vedrørende brud på persondatasikkerheden	-	1	0

Påtaler/påbud/kritik fra Datatilsynet	Tilsyn 2: Datatilsynet udtalte alvorlig kritik af kommunen.	0	0
Bøder fra Datatilsynet	0	0	0

Interne kontroller i kommunen med overholdelse af GDPR

Antal	2020	2021	**2022**
Planlagte tilsyn	0	0	4
Emne for planlagt tilsyn			Generelt tilsyn med enheder, herunder gennemgang af 2-3 arbejdsgange i relation til GDPR med medarbejdere
Gennemførte tilsyn			4
Emne for gennemført tilsyn			Generelt tilsyn med enheder, herunder gennemgang af 2-3 arbejdsgange i relation til GDPR med medarbejdere

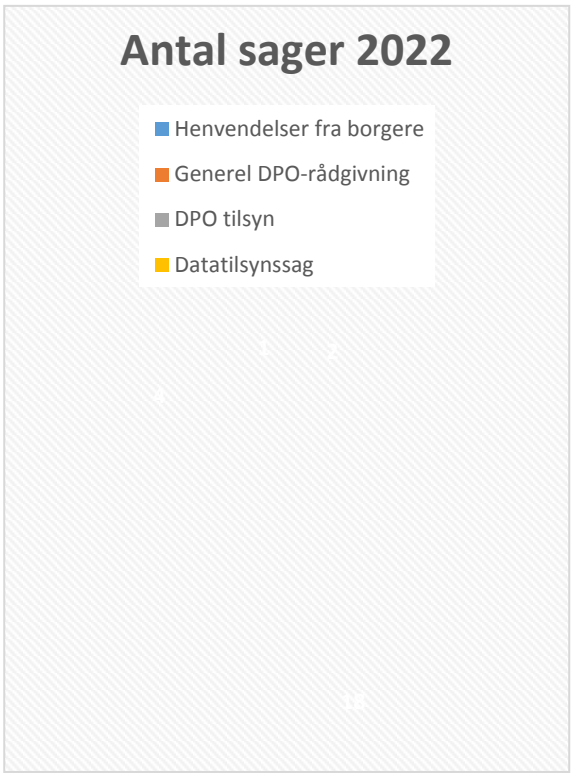
Kommunens GDPR-ressourcer

Antal	2020	2021	**2022**
Dedikerede årsværk til implementering og drift af GDPR	2	3	2
Øvrige årsværk til implementering og drift af GDPR	6	6	6

Bilag 3 – Sagsstatistik

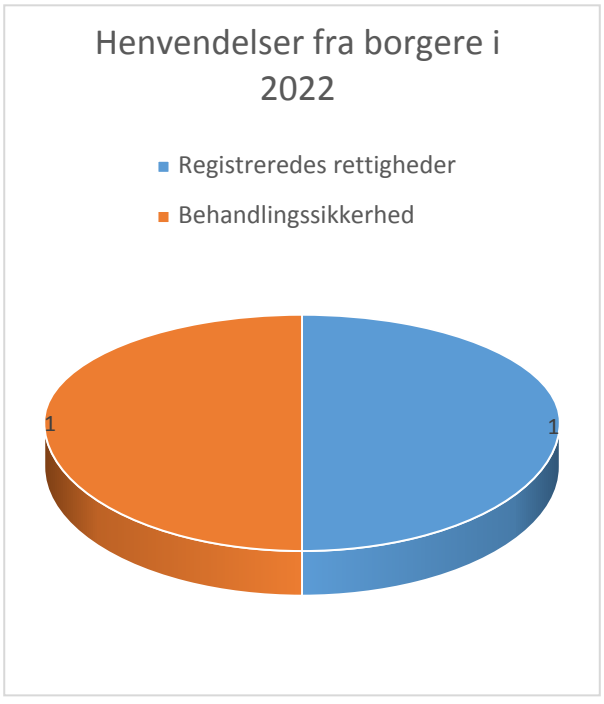
Antal sager

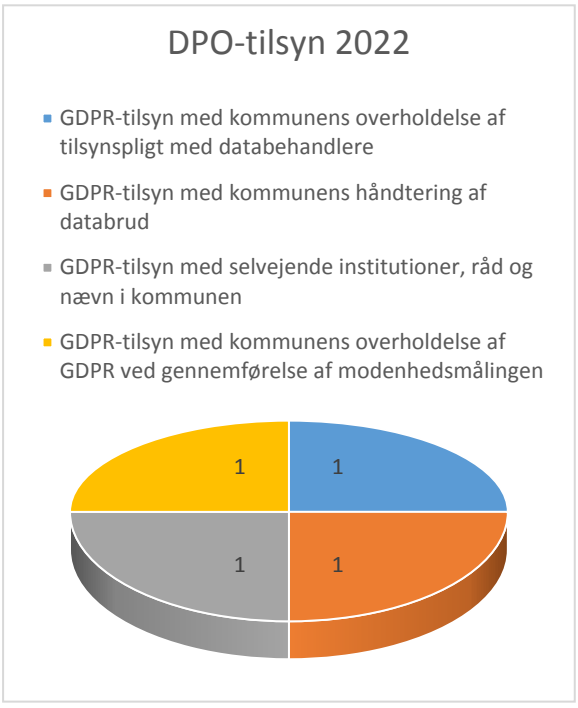
DPO'en har i perioden 1. januar 2022 til og med 31. december 2022 oprettet i alt 24 sager, som er fordelt på sagskategorierne: henvendelser fra borgere, generel DPO-rådgivning, samt DPO-tilsyn, som omfatter DPO'ens tilsyn med kommunen. Derudover er der oprettet 1 sag, hvor kommunen har været i kontakt med Datatilsynet. I 2022 var den kontakt deltagelse i en skriftlig modenhedsmåling hos Datatilsynet.



Forespørgsler fra kommunen

Henvendelser fra borgere og DPO-tilsyn





Møder i 2022

Med Covid-19 kategoriseret som et mindre problem, har DPO'en kunnet besøge kommunerne fysisk igen. Der er løbende fastholdt regelmæssig deltagelse i onlinemøder (såkaldte GDPR-fortolkningsmøder) for sikkerhedskoordinatorerne fra kommunerne i Den Storkøbenhavnske Digitaliseringsforening.

Leverancer

DPO'en har i 2022 brugt meget arbejde på at følge og dokumentere, samt facilitere viden om brugen af Google Workspace til skolerne i DSD efter sommerferien 2022, hvor Helsingør kommune fik et forbud mod brugen af systemet og det efterfølgende forløb med hhv. KL, Kombit, Google og Datatilsynet.
DPO'en følger desuden meget tæt Kombits udmelding om aftale med Amazon Web Services omkring AULA, hvor der løbende er kommunikation omkring afklaringen.
DPO'en har lavet analyser af og kommenteret på løsningen KL Gateway, som KL har forsøgt sat i brug vha. teknologi fra FUT-projektet.

Leverancer 2022

- ✓ Opfølgning, dokumentation og rådgivning for arbejdet med Cloud services. Herunder specifikt Google, Amazon og Microsoft.
- ✓ Vurderinger og kommentarer til konsekvensanalyser på systemet KL Gateway.
- ✓ Udsendelse af det månedlige DSD Nyhedsbrev