DATABESKYTTELSESRÅDGIVERENS ÅRSRAPPORT 2018-2019

Afsender:

Databeskyttelsesrådgiveren

Modtager:

Kommunalbestyrelsen i Ishøj Kommune

Indhold

Årsrapport 2018-2019

Den 25. maj 2018 var et skelsættende øjeblik i databeskyttelsesretten. Fra denne dato fik de nye EU-regler om databeskyttelse virkning i Danmark og i de øvrige lande i Den Europæiske Union. Reglerne kaldes i daglig tale GDPR, der står for The General Data Protection Regulation. Reglerne gælder for Ishøj Kommune.

Formålet med GDPR er at beskytte de borgere, som der behandles persondata om. Reglerne skal bl.a. sikre borgernes ret til privatliv og skabe tillid til håndtering og behandling af persondata om borgerne.

GDPR bygger videre på regler, som allerede fulgte af den tidligere persondatalov, men GDPR indeholder også mange nyskabelser, der har til formål at styrke beskyttelse af persondata.

En nyskabelse er kravet om, at kommunen skal have en databeskyttelsesrådgiver, som har til opgave at underrette og rådgive kommunen om de databeskyttelsesretlige pligter, at overvåge overholdelsen af databeskyttelsesretlige regler i kommunen, at rådgive kommunen om konsekvensanalyser, at samarbejde med Datatilsynet og fungere som kontaktpunkt for Datatilsynet og for borgerne.

En anden nyskabelse er kravet om, at efterlevelse af GDPR skal kunne påvises af kommunen (det såkaldte ansvarlighedsprincip), hvilket medfører et dokumentationskrav for kommunen.

En tredje nyskabelse er det forhold, at der er mulighed for at give bøder på op til 16 mio. kr. til kommuner og andre offentlige myndigheder for manglende efterlevelse af GDPR.

Denne årsrapport, som er den første af sin slags fra kommunens databeskyttelsesrådgiver, dækker perioden 25. maj 2018 – 31. december 2019.

Formålet med årsrapporten er at rapportere til kommunens øverste politiske ledelse om modenhedsniveauet og status for efterlevelse af GDPR i Ishøj Kommune samt at give anbefalinger for kommunens arbejde med databeskyttelse i 2020.

I rapportens ledelsesresumé er der en opsamling vedrørende modenhedsniveauet og status for efterlevelse af GDPR i Ishøj Kommune samt databeskyttelsesrådgiverens anbefalinger til kommunen.

Bilag 1 indeholder oplysninger om en GDPR-modenhedsmåling af kommunen foretaget i juni måned 2019.

Bilag 2 indeholder nøgletal fra kommunen om overholdelse af GDPR. Nøgletallene er indsamlet og opgjort i slutningen af 2019.

Bilag 3 indeholder sagsstatistik for databeskyttelsesrådgiverens arbejde i perioden.

Daniel Soelberg Bach

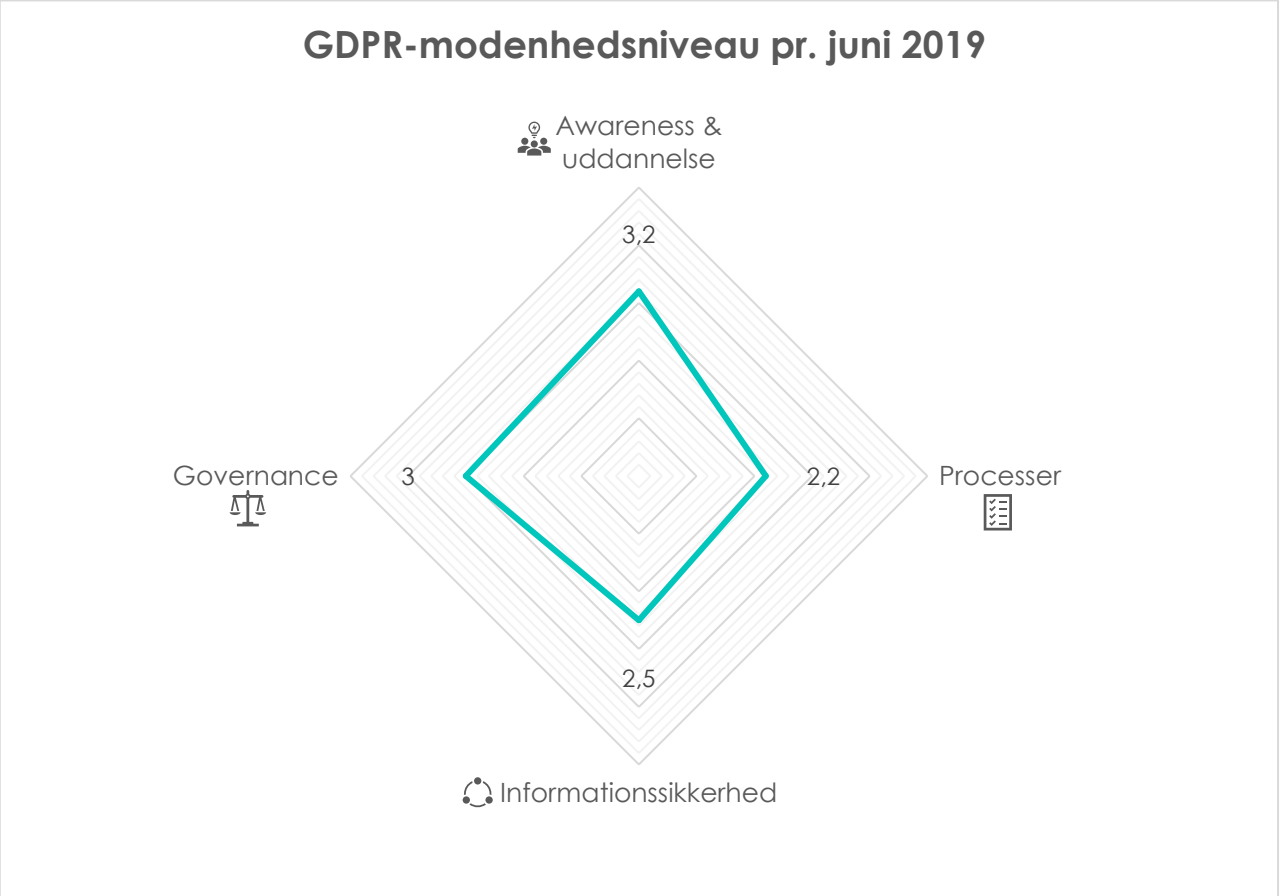
Databeskyttelsesrådgiver, Ishøj Kommune, 12. marts 2020.

Ledelsesresumé

GDPR-modenhedsniveau i kommunen

I juni 2019 gennemførte databeskyttelsesrådgiveren en såkaldt GDPR-modenhedsmåling som led i databeskyttelsesrådgiverens lovpligtige opgave med at overvåge efterlevelsen af GDPR i Ishøj Kommune. GDPR-modenhedsmålingen omfattede 40 modenhedskriterier (herefter kriterier), som afspejler lovkrav efter GDPR eller andre forhold af betydning for efterlevelse af GDPR. Målingen er baseret på en skala fra 1-5, hvor modenhedsniveau 1 er lavest og 5 er højest (niveau 1-2 indikerer, at kommunen ikke efterlever GDPR, niveau 3 indikerer, at kommunen delvist efterlever GDPR. Niveau 4-5 indikerer, at kommunen efterlever GDPR).

I den følgende model præsenteres resultaterne af GDPR-modenhedsmålingen fordelt på fire hovedområder, hvorunder de 40 kriterier er placeret. Resultaterne fordelt på de enkelte kriterier foreligger i detaljeret form i bilag 1



Kommunens gennemsnitlige GDPR-modenhedsniveau var 2,5 på tidspunktet for målingen.

Resultatet viser, at Ishøj Kommunes GDPR-modenhedsniveau var lavere end modenhedsniveau 3 for mange kriterier, som afspejler opfyldelse af krav direkte efter GDPR. Dette indikerer, at Ishøj Kommune på tidspunktet for målingen ikke efterlevede de krav efter GDPR, som de pågældende kriterier afspejler. At ligge på det pågældende modenhedsniveau i forhold til de pågældende kriterier medfører, at der i nogle tilfælde kan være en risiko for, at kommunen kan få kritik eller bøder fra Datatilsynet, hvis tilsynet fører tilsyn med kommunens efterlevelse af de pågældende krav efter GDPR. Forholdet medfører også, at der i nogle tilfælde kan være risiko for, at persondata i kommunen ikke beskyttes i tilstrækkeligt omfang – og dermed kan der være risiko for, at borgernes rettigheder (retten til databeskyttelse og retten til beskyttelse af privatlivets fred) ikke beskyttes.

På området **governance** (dvs. ledelse og styring) viste målingen bl.a., at kommunens modenhedsniveau var lavt (niveau 2) i forhold til kriteriet ledelsesmæssig understøttelse af overholdelse af GDPR. Modenhedsniveauet var højere (niveau 3 eller højere) i forhold til bl.a. kriterierne roller og ansvar (dvs. fordeling af ansvar og roller for efterlevelse af GDPR) databeskyttelsespolitikker (dvs. interne regler om beskyttelse af persondata), opdatering af databeskyttelsespolitikker samt kommunikation af databeskyttelsespolitikker. I kommunens enheder var der et lavt modenhedsniveau (gennemsnitsniveau 2,7) i forhold til kriteriet styring og rapportering omkring efterlevelse af GDPR. Det laveste modenhedsniveau (gennemsnitsniveau 2,6) i kommunens enheder var i forhold til kriteriet ressourcer til arbejdet med overholdelse af GDPR.

På området for **awareness og uddannelse** viste målingen, at kommunens modenhedsniveau var højt (niveau 4) i forhold til kriteriet awareness (dvs. information til medarbejdere og ledelse om beskyttelse af persondata i kommunen). Kommunens modenhedsniveau var lavere (gennemsnitsniveau 2,4) i forhold til kriteriet uddannelse (dvs. uddannelse/træning af medarbejdere og ledere om beskyttelse af persondata).

På området for **processer** viste målingen bl.a., at der i kommunens enheder – med få positive udsving – var et lavt modenhedsniveau (under niveau 3) i forhold til kriterier, som afspejler grundlæggende behandlingsprincipper efter GDPR (dvs. dataminimering, datakvalitet, formålsbegrænsning og opbevaringsbegrænsning). Det laveste modenhedsniveau i kommunens enheder var i forhold til kriteriet oplysningspligt (dvs. skriftlig information til borgerne ved kommunens indsamling af persondata om borgerne), hvor gennemsnitsniveauet var 2,3. Der var også - med få positive udsving - et lavt modenhedsniveau (niveau 2 eller lavere) i kommunen i forhold til kriterier, som afspejler krav efter GDPR om håndtering af databehandlere (dvs. bl.a. register for databehandlere, kvalitetssikring af databehandleren, procedure for tilsyn med databehandleren samt gennemførelse af tilsyn med databehandlere). Modenhedsniveauet var også lavt (niveau 2 eller lavere) i forhold til kriterier, som afspejler krav efter GDPR om risikostyring (dvs. risikovurderinger efter GDPR med fokus på identificering af risici for borgerne ved tab af fortrolighed, integritet og tilgængelighed for persondata i kommunen samt implementering af passende sikkerhedsforanstaltninger, som sikrer et passende sikkerhedsniveau for persondata i kommunen, herunder procedure for stillingtagen til gennemførelse af konsekvensanalyser (såkaldt DPIA), procedure for afprøvning af sikkerhedsforanstaltningernes effektivitet (såkaldt sikkerhedstest) samt retningslinjer der sikrer, at nye it-systemer er designet/bygget og eksisterende systemer er indstillet således, at systemerne beskytter persondata og efterlever reglerne i GDPR (såkaldt privacy by design og privacy by default).

På området for **informationssikkerhed** var der et lavt modenhedsniveau (niveau 2) i forhold til kriteriet sikkerhedsprogram ISO27001 (dvs. et program som sikrer, at principperne i sikkerhedsstandarden ISO27001 følges). Modenhedsniveauet var også lavt (niveau 2) i forhold til kriteriet risikovurdering og sikkerhedsforanstaltninger ISO27001 (dvs. forretningsorienteret risikovurdering og sikkerhedsforanstaltninger). Modenhedsniveauet var højere (niveau 4) i forhold til kriteriet beredskabsplan (dvs. plan og procedure i kommunen for videreførelse af kritiske forretningsprocesser i tilfælde af kritiske situationer (f.eks. ved omfattende hackerangreb), mens modenhedsniveauet var lavt (niveau 2) forhold til kriteriet test af beredskabsplan.

Nøgletal fra kommunen om overholdelse af GDPR

Nøgletallene fra kommunen om overholdelse af GDPR (se bilag 2) viser, at kommunen har håndteret langt hovedparten af anmodningerne fra borgere (38 ud af 40 anmodninger), som har gjort brug af deres rettigheder efter GDPR, inden for 30-dages fristen efter GDPR. Tallene viser

desuden, at kommunen har håndteret langt hovedparten af persondatasikkerhedsbrud (20 ud af 22), som er anmeldt til Datatilsynet, inden for 72-timers fristen efter GDPR. Kommunen har også været opmærksom på at underrette borgerne i tilfælde af persondatasikkerhedsbrud, hvis dette er vurderet relevant.

Nøgletallene viser, at kommunen ikke har inddraget databeskyttelsesrådgiveren i forbindelse med anskaffelser af nye it-systemer/løsninger til brug for behandling af persondata. Det er et krav efter GDPR, at kommunen skal inddrage databeskyttelsesrådgiveren i alle spørgsmål vedrørende beskyttelse af persondata. Det betyder bl.a., at databeskyttelsesrådgiveren i god tid og på et tilstrækkeligt grundlag skal inddrages ved anskaffelser af nye it-systemer til brug for behandling af persondata i kommunen. Dette gælder navnlig i forhold til it-systemer, som skal bruges til behandling af følsomme persondata.

Kommunen har heller ikke inddraget databeskyttelsesrådgiveren i processer for anskaffelse af it-systemer til brug for behandling af persondata før offentliggørelse af udbudsmateriale, hvor kommunen skal sikre, at nye it-systemer fra start er designet/bygget således, at systemerne beskytter persondata samt efterlever GDPR (privacy by design).

Kommunens nøgletal viser derudover, at kommunen kun i begrænset omfang (en gang) har gennemført stikprøve af efterlevelse af GDPR i kommunen, og kommunen har heller ikke gennemført konsekvensanalyser (DPIA), som påkrævet efter GDPR i forhold til nye eller ændrede behandlinger, som sandsynligvis vil indebære en høj risiko for borgernes rettigheder og frihedsrettigheder (der henvises i øvrigt til bilag 2 for en uddybning af nøgletallene).

Databeskyttelsesrådgiveren har i medio 2018 foretaget et tilsyn med efterlevelse af samtykkekrav efter GDPR i Ishøj Svømmehal i forhold til indsamling og behandling af persondata om svømmehallens brugere. Tilsynet identificerede mangler i svømmehallens samtykkeerklæring, som var utilstrækkelig til at indhente et gyldigt samtykke fra svømmehallens brugere til indsamling og behandling af brugernes persondata. Samtykkeerklæringen informerede ikke i tilstrækkelig grad svømmehallens brugerne om formålene med den behandling, som svømmehallen skulle bruge persondata til, ligesom brugerne ikke havde mulighed for at til- eller fravælge hvilke formål, brugerne reelt ønskede at give deres samtykke til. De af svømmehallen indhentede samtykker fra svømmehallens brugere udgjorde således ikke et gyldigt behandlingsgrundlag for svømmehallens indsamling og behandling af persondata om svømmehallens brugerne. Databeskyttelsesrådgiveren konstaterede i forbindelse med en opfølgning i ultimo 2019, at Ishøj Svømmehals samtykkeerklæring fortsat ikke i fuldt omfang efterlevede GDPR-samtykkekrav.

Status primo 2020

Det er samlet set databeskyttelsesrådgiverens opfattelse, at der har været en positiv udvikling i Ishøj Kommune siden GDPR-modenhedsmålingen blev foretaget i juni 2019. Databeskyttelsesrådgiveren lægger i den forbindelse vægt på, at kommunen har et igangværende kortlægningsprojekt for dokumentation af alle behandlinger af persondata i kommunen (såkaldt fortegnelser over behandlingsaktiviteter), hvilket kommunen kan anvende som en løftestang til at få et overblik over behandlingerne af persondata i kommunen samt til at øge GDPR-modenhedsniveauet og efterlevelsen af GDPR. Databeskyttelsesrådgiveren lægger desuden vægt på, at kommunen efter GDPR-modenhedsmålingen i juni 2019 har etableret en nedskrevet procedure for indgåelse af databehandleraftaler med henblik på efterlevelse af GDPR-krav herom. Kommunen har også sikret en yderligere forankring af roller og ansvar i kommunen vedrørende udførelse af GDPR-opgaver i kommunen, ligesom der i kommunen er truffet beslutning om at opkvalificere medarbejdere, som skal udføre GDPR-opgaver i kommunen.

Kommunen har i perioden 2018-2019 haft et dedikeret årsværk (fordelt på mange personer) til arbejdet med implementering og drift af GDPR. Der er efter databeskyttelsesrådgiverens vurdering – trods den ovennævnte positive udvikling - brug for flere ressourcer til implementering og drift af GDPR i kommunen for at øge kommunens modenhedsniveau, da GDPR-

modenhedsmålingen viste, at kommunen har et stort arbejde foran sig med udarbejdelse af bl.a. nedskrevne procedurer for sikring af overholdelse af behandlingsprincipper (særlig opbevaringsbegrænsning) samt procedure for oplysningspligt, ligesom kommunen vil skulle bruge ressourcer til løbende håndtering af databehandlere (bl.a. gennemførelse af tilsyn med databehandlere) samt ressourcer til løbende risikostyring (gennemførelse af risikovurderinger efter GDPR og implementering af sikkerhedsforanstaltninger på grundlag af risikovurderinger efter GDPR). Dertil kommer, at kommunen vil skulle gennemføre flere stikprøver af overholdelse af databeskyttelsespolitikker og GDPR i kommunen samt gennemføre konsekvensanalyser, når dette er påkrævet, for at efterleve GDPR.

Anbefalinger

Databeskyttelsesrådgiveren anbefaler kommunen at tilføre databeskyttelsesområdet flere ressourcer til arbejdet med implementering og drift af GDPR i kommunen.

Databeskyttelsesrådgiveren anbefaler desuden kommunen at fokusere på at øge GDPR-modenhedsniveauet til minimum niveau 3 for så vidt angår modenhedskriterier, som afspejler krav direkte efter GDPR.

Kommunen bør navnlig prioritere at øge GDPR-modenhedsniveauet for modenhedskriterierne vedrørende:

- Uddannelse/træning (i de enheder, hvor uddannelse var på et lavt niveau)
- Procedurer for efterlevelse af behandlingsprincipper efter GDPR (navnlig princippet om opbevaringsbegrænsning)
- Risikostyring (gennemførelse af risikovurderinger efter GDPR og implementering af passende sikkerhedsforanstaltninger efter GDPR)
- Retningslinjer som sikrer, at nye it-systemer og eksisterende systemer beskytter persondata og efterlever GDPR (privacy by design og privacy by default)

Databeskyttelsesrådgiveren anbefaler herudover kommunen at inddrage databeskyttelsesrådgiveren ved anskaffelse af nye it-systemer/løsninger til brug for behandling af persondata, herunder i udarbejdelse af kravspecifikationer før offentliggørelse af udbudsmaterialer med henblik på at sikre, at systemerne beskytter persondata og efterlever GDPR. Dette gælder navnlig i forhold til nye it-systemer/løsninger til brug for behandling af følsomme persondata i kommunen. Databeskyttelsesrådgiveren anbefaler endelig kommunen at fokusere på at gennemføre konsekvensanalyser før behandling af persondata i nye it-systemer/løsninger, hvis behandlingen sandsynligvis vil indebære høje risici for borgernes rettigheder og frihedsrettigheder, herunder sørge for at inddrage databeskyttelsesrådgiveren i tilfælde hvor kommunen måtte være tvivl om, hvorvidt en konsekvensanalyse er påkrævet.

Bilag 1

GDPR-modenhedsmåling af kommunen

Formål

GDPR-modenhedsmålingen af kommunen i juni 2019 blev udført som en del af databeskyttelsesrådgiverens lovpligtige opgave med at føre tilsyn med/overvåge overholdelsen af de databeskyttelsesretlige regler i kommunen.

Formålet med at gennemføre en GDPR-modenhedsmåling er at måle niveauet for efterlevelse af GDPR i kommunen samt at skabe læring og understøtte kommunen i forhold til arbejdet med implementering og drift af GDPR.

Metode

Målingen af GDPR-modenhed er baseret på principper fra den anerkendte IACPA Privacy Maturity Model[1]. Databeskyttelsesrådgiveren har modificeret modellens kriterier til kommunal kontekst med primær fokus på GDPR. Data til brug for målingen er baseret på en survey af respondenter, som kommunen har udpeget til at besvare for kommunen (selvevaluering).

For at sikre kvalitet i de indsamlede data har databeskyttelsesrådgiveren gennemført to workshops i kommunen for de udpegede respondenter, hvor respondenterne har haft mulighed for at besvare surveyen, og hvor databeskyttelsesrådgiveren har guidet respondenterne gennem modenhedskriterierne og svaret på spørgsmål mv.

Hvert modenhedskriterium, som der er målt på, afspejler krav direkte efter GDPR eller andre forhold af betydning for GDPR og informationssikkerhed. Hvert kriterium indeholder fem udsagn (svarende til modenhedsniveau 1-5) med beskrivelse af aktiviteter, dokumentation, procedurer og andre oplysninger, som forventes til hvert modenhedsniveau. Respondenterne er instrueret om at vælge udsagn, som er mest retvisende for status for GDPR-modenhed i kommunen. Respondenternes valg af udsagn definerer GDPR-modenhedsniveauet for hvert målte modenhedskriterium. Databeskyttelsesrådgiveren har verificeret respondenters besvarelser af surveyen, hvis det er skønnet relevant.

Det er tilsigtet, at hvert fagområde indeholder flere besvarelser. Ishøj Kommune har udpeget kommunens niveau 3 ledere som respondenter i enhederne, så hver enhed/driftssted deltager i modenhedsmålingen. Det vil sige, at modenhedskriterierne for fagområderne måles på en gennemsnitsberegning fra besvarelserne fra de udpegede respondenter i enhederne. Modenhedskriterierne for hver enkelt enhed beregnes derimod på grundlag af hver respondents vurdering på vegne af enheden.

Omfang

Der er foretaget en måling på baggrund af en række modenhedskriterier i IT- og Digitalisering i Ishøj Kommune. Og der er foretaget en måling af andre modenhedskriterier i hver af Ishøj Kommunes udpegede enheder.

Modenhedskriterier

Modenhedskriterierne hører under fire områder (kriterier med * afspejler krav direkte efter GDPR):

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

Governance

1. Ledelsesmæssig understøttelse
2. Roller og ansvar*
3. Databeskyttelsespolitikker*
4. Opdatering af databeskyttelsespolitikker*
5. Kommunikation af databeskyttelsespolitikker
6. Kendskab til kommunens politikker*
7. Monitorering af overholdelse af politikker*
8. Monitorering af lovgivningsområder
9. Årshjul for GDPR-arbejdsopgaver
10. Styring og rapportering
11. Ressourcer til GDPR-arbejde

Awareness og uddannelse

12. Awareness*
13. Uddannelse*

Processer

14. Fortegnelse*
15. Indsamling til sagligt formål (dataminimering)*
16. Datakvalitet*
17. Formålsbegrænsning*
18. Opbevaringsbegrænsning*
19. Samtykke efter GDPR*
20. Oplysningspligt*
21. Håndtering af registreredes (borgernes) rettigheder*
22. Persondatasikkerhedsbrud*
23. Klager fra registrerede (borgerne)
24. Register for databehandlere*
25. Kvalitetssikring af databehandlere (due diligence)*
26. Kvalitetssikring af databehandleraftaler*
27. Indgåelse af databehandleraftaler*
28. Procedure for tilsyn med databehandlere*
29. Tilsyn med databehandlere*
30. Risikovurderinger efter GDPR*
31. Implementering af sikkerhedsforanstaltninger*
32. DPIA (konsekvensanalyser)*
33. Sikkerhedstest*
34. Adgangsstyring til persondata*
35. Inddragelse af databeskyttelsesrådgiveren*
36. Privacy by design og privacy by default*

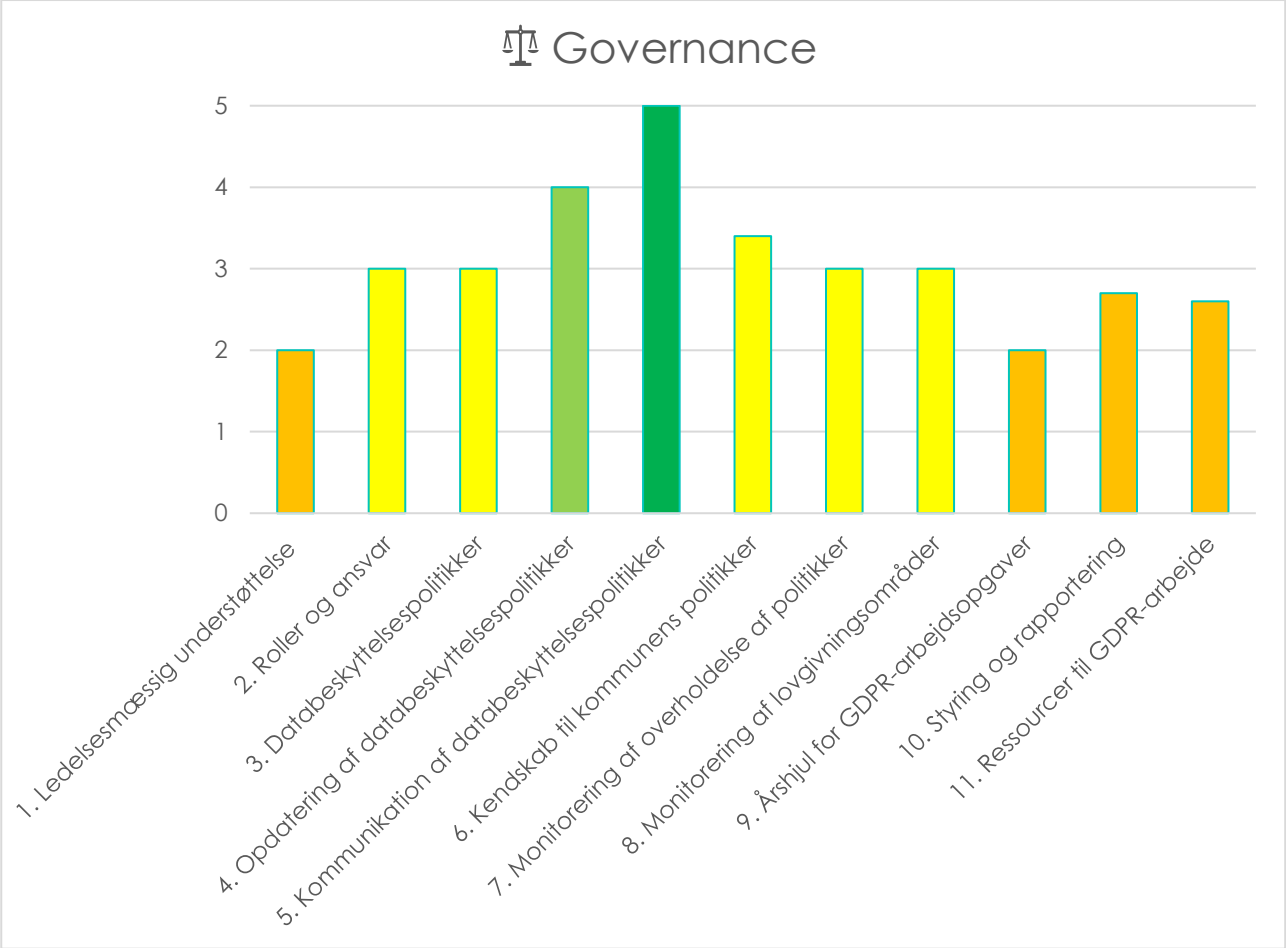
Informationssikkerhed

37. Sikkerhedsprogram (ISO27001)
38. Risikovurderinger og sikkerhedsforanstaltninger (ISO27001)
39. Beredskabsplan
40. Test af beredskabsplan

Skala

Niveau	Beskrivelse	Efterlevelse af GDPR
1	Efterlevelse af GDPR er ikke på plads	
2	Delvist indført og dokumenteret	
3	Indført og veldokumenteret	
4	Implementeret i fuldt omfang	
5	Implementeret i fuldt omfang, optimering og forbedring af processer.	

Modenhedsniveau 1-2 indikerer, at kommunen ikke efterlever GDPR. Niveau 3 indikerer, at kommunen delvist efterlever GDPR. Modenhedsniveau 4-5 indikerer, at kommunen efterlever GDPR. Terminologien "indikation" på ikke efterlevelse af GDPR, "indikation" på delvis efterlevelse af GDPR samt "indikation" på efterlevelse af GDPR samt ikonerne i højre kolonne ovenfor skal ses i lyset af, at GDPR-modenhedsmålingen ikke er baseret på databeskyttelsesrådgiverens vurdering af skriftlig dokumentation fra kommunen, men på en selvevaluering af udpegede respondenter fra kommunen.



1. Ledelsesmæssig understøttelse

Kriteriet ledelsesmæssig understøttelse afspejler ikke et krav direkte efter GDPR, men ledelsesmæssigt engagement og understøttelse er afgørende for implementering og drift af GDPR i organisationen. Direktion og ledelse bør understøtte overholdelse af krav efter GDPR i organisationen ved at kommunikere klart og tydeligt i organisationen om vigtigheden af at overholde krav efter GDPR.

Kommunens GDPR-modenhed i forhold til dette kriterium var på niveau 2.

2. Roller og ansvar

Roller og ansvar er et kriterium, som afspejler krav direkte efter GDPR, hvorefter roller og ansvar for overholdelse af GDPR skal være tydeligt defineret i organisationen ved udspecificering af væsentlige roller og ansvar for overholdelse af GDPR.

GDPR-modenhed i kommunen i forhold kriteriet var på niveau 3

3. Databeskyttelsespolitikker

Kriteriet databeskyttelsespolitikker afspejler et krav direkte efter GDPR, hvorefter der skal være interne databeskyttelsespolitikker i organisationen, som beskriver, hvordan ledere og medarbejdere skal håndtere og beskytte persondata i organisationen. Politikkerne skal indeholde interne regler for organisationens ledere og medarbejdere, som sikrer overholdelse af GDPR og beskyttelse af persondata.

Kommunens GDPR-modenhed i forhold til kriteriet var på niveau 3.

4. Opdatering af databeskyttelses-politikker

Opdatering af databeskyttelsespolitikker er et kriterium, som afspejler et krav direkte efter GDPR, hvorefter organisationen skal sikre, at interne databeskyttelsespolitikker er opdateret.

Kommunens modenhedsniveau i forhold til dette kriterium var på niveau 4.

5. Kommunikation af databeskyttel-sespolitikker

Kommunikation af kommunens interne databeskyttelsespolitikker er et modenhedskriteriet, som ikke afspejler krav direkte efter GDPR. Der er målt på kriteriet, fordi kommunikation af databeskyttelsespolitikker til ledere og medarbejdere i organisationen er afgørende for at sikre kendskab til databeskyttelsespolitikker i organisationen.

GDPR-modenheden i kommunen i forhold til dette kriterium var på niveau 5.

6. Kendskab til politikker

Kriteriet kendskab til databeskyttelsespolitikker afspejler et krav direkte efter GDPR, hvorefter ledere og medarbejdere i organisationen skal have kendskab til interne databeskyttelsespolitikker i organisationen.

Kommunens GDPR-modenhed i forhold til kriteriet var på niveau 3,4 (her gennemsnit af enhedernes besvarelser).

7. Monitorering af overholdelse af politikker

Kriteriet monitorering af overholdelse af databeskyttelsespolitikker afspejler et krav direkte efter GDPR, hvorefter organisationen skal monitorere overholdelse af interne politikker om databeskyttelse – og dermed monitorere organisationens overholdelse af GDPR.

Kommunens GDPR-modenhed i forhold til kriteriet var på niveau 3.

8. Monitorering af lovområder

Kriteriet monitorering af lovgivningsområder afspejler ikke et krav direkte efter GDPR. Der er målt på kriteriet i målingen, fordi ændringer i lovgivning kan påvirke databeskyttelsespolitikker i organisationen.

GDPR-modenhed i kommunen i forhold til kriteriet var på niveau 3.

9. Årshjul for GDPR-opgaver

Kriteriet årshjul for GDPR-opgaver afspejler ikke et direkte krav efter GDPR. Der er målt på kriteriet, fordi et årshjul kan understøtte udførelse af GDPR-opgaver i organisationen.

GDPR-modenhed i kommunen i forhold til dette kriterium var på niveau 2.

10. Styring og rapportering

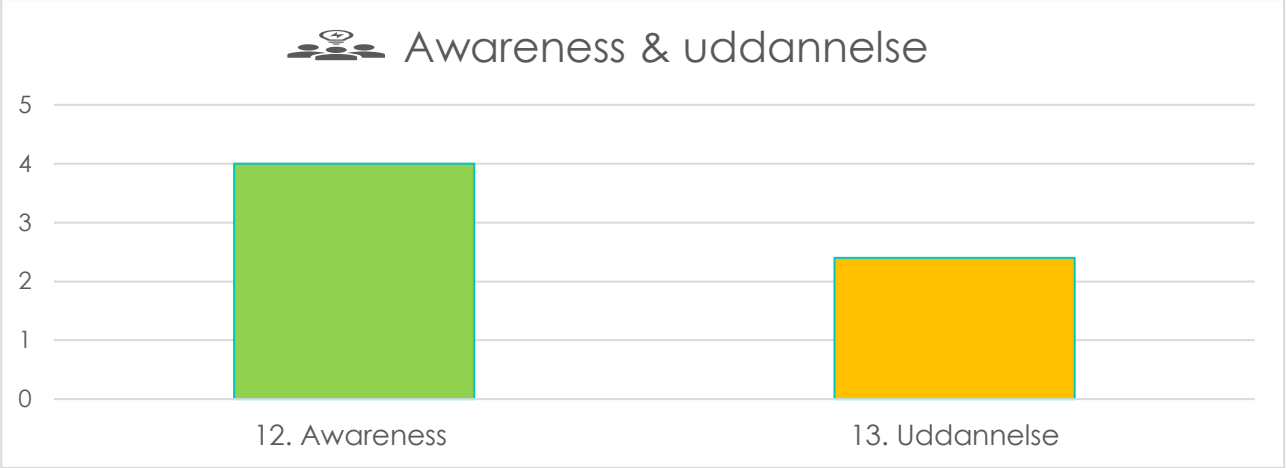
Styring og rapportering er et kriterium, som ikke afspejler et krav direkte efter GDPR. Der er målt på kriteriet, fordi kriteriet har betydning for implementering og drift af GDPR i enhederne i organisationen

Kommunens GDPR-modenhed var på niveau 2,7 (her gennemsnit af enhedernes besvarelser).

11. Ressourcer til GDPR-arbejde

Ressourcer til GDPR-arbejde er ikke et kriterium, som afspejler et krav direkte efter GDPR, men tilstrækkelige ressourcer (f.eks. medarbejdere, tekniske løsninger og konsulenter) i enhederne i en organisation er ikke desto mindre en forudsætning for overholdelse af GDPR i organisationen.

GDPR-modenhed i kommunen i forhold til kriteriet var på niveau 2,6 (her gennemsnit af enhedernes besvarelser).



12. Awareness

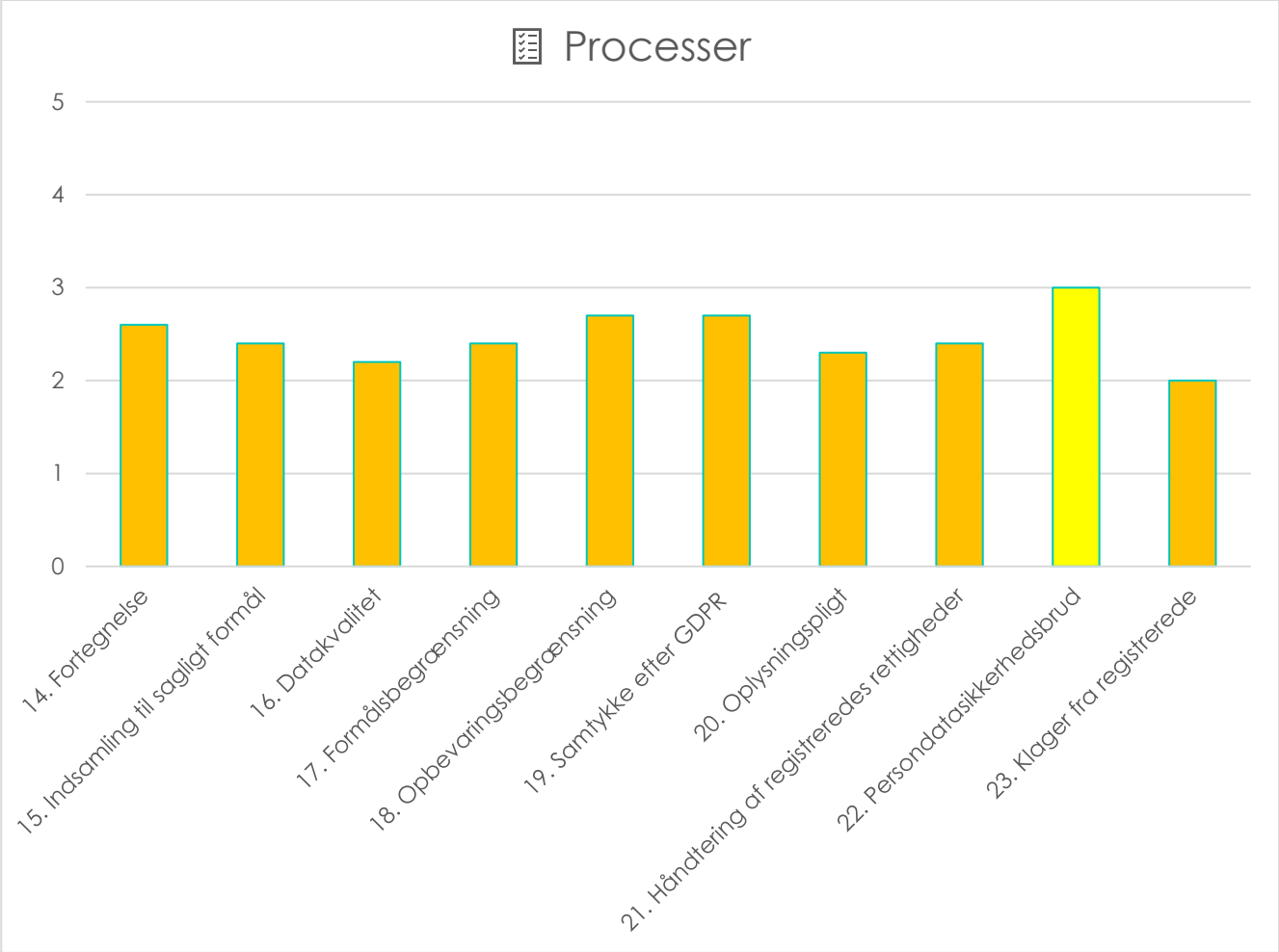
Kriteriet awareness afspejler et krav direkte efter GDPR, hvorefter ledere og medarbejdere i organisationen løbende skal informeres om beskyttelse af persondata for at skabe opmærksomhed og varsomhed omkring beskyttelse af persondata i organisationen.

Kommunes GDPR-modenhed i forhold til kriteriet var på niveau 4.

13. Uddannelse

Uddannelse er også et kriterium, som afspejler et krav direkte efter GDPR, hvorefter ledere og medarbejdere i organisationens fagområder løbende skal uddannes (fx kurser, oplæring, træning) i overholdelse af bestemmelser i GDPR og beskyttelse af persondata.

GDPR-modenhed i kommunen i forhold til dette kriterium var på niveau 2,4 (her gennemsnit af enhedernes besvarelser).



14. Fortegnelse

Fortegnelse er et kriterium, som afspejler et krav direkte efter GDPR, hvorefter der skal føres fortegnelse over behandlinger af persondata (såkaldt fortegnelse over behandlingsaktiviteter) i organisationen.

Kommunens GDPR-modenhed i forhold til kriteriet var på niveau 2,6 (her gennemsnit af enhedernes besvarelser).

Introduktion til behandlingsprincipper efter GDPR

Det følger af GDPR, at enhver behandling af persondata i organisationen skal være i overensstemmelse med behandlingsprincipperne efter GDPR. Behandlingsprincipperne handler grundlæggende om, at organisationen kun må indsamle persondata til sagligt formål, at persondata skal være korrekte, at behandling af persondata skal begrænses til det formål, hvortil persondata blev indsamlet (formålsbegrænsning) kun og at persondata ikke må opbevares i længere tid, end nødvendigt (opbevaringsbegrænsning). Organisationen skal kunne påvise efterlevelsen af behandlingsprincipperne, jf. ansvarlighedsprincippet, hvilket i udgangspunktet forudsætter dokumentation i form af nedskrevne procedurer, som sikrer efterlevelse af behandlingsprincipperne i organisationen. I GDPR-modenhedsmålingen har databeskyttelsesrådgiveren gennemført en måling i enhederne af, om der foreligger nedskrevne procedurer, som sikrer efterlevelse af behandlingsprincipper efter GDPR.

15. Indsamling til sagligt formål

Kriteriet afspejler et direkte krav efter GDPR, hvorefter organisationen skal sikre (ved nedskrevne procedurer), at der kun indsamles persondata til sagligt formål og kun

indsamles persondata, som er nødvendige af hensyn til formålet.

Kommunens GDPR-modenhed i forhold til kriteriet var på niveau 2,4 (her gennemsnit af enhedernes besvarelser).

16. Datakvalitet

Kriteriet afspejler et direkte krav efter GDPR, hvorefter organisationen skal sikre (ved nedskrevne procedurer), at de behandlede persondata er korrekte, og at persondata, som måtte være fejlagtige rettes eller slettes straks.

GDPR-modenhed i kommunen i forhold til kriteriet var på niveau 2,2 (her gennemsnit af enhedernes besvarelser).

17. Formålsbegrænsning

Kriteriet afspejler et direkte krav efter GDPR, hvorefter organisationen skal sikre (ved nedskrevne procedurer), at persondata ikke behandles (læs viderebehandles/genbruges) på en måde, som er uforeneligt med det formål, hvortil persondata i første omgang blev indsamlet.

Kommunens GDPR-modenhed i forhold til kriteriet var på niveau 2,4 (her gennemsnit af enhedernes besvarelser).

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

18. Opbevaringsbegrænsning

Kriteriet afspejler et direkte krav efter GDPR, hvorefter organisationen (ved nedskrevet procedure) skal sikre, at persondata ikke opbevares i længere tid end nødvendigt for opfyldelse af det formål, som persondata i første omgang blev indsamlet til.

GDPR-modenhed i kommunen i forhold til kriteriet var på niveau 2,7 (her gennemsnittet af enhedernes besvarelser).

19. Samtykke efter GDPR

Samtykke efter GDPR er et kriterium, som afspejler et krav direkte efter GDPR, hvorefter persondata, som behandles på grundlag af samtykke efter GDPR, forudsætter, at samtykket er gyldigt, hvilket organisationen skal kunne påvise, jf. ansvarlighedsprincippet. Dette forudsætter, at der er nedskrevet procedurer, som sikrer indsamling af gyldigt samtykke fra borgerne. Der er kun målt på kriteriet i de fagområder, som har svaret bekræftende på, at der behandles persondata på grundlag af samtykke efter GDPR.

Kommunens GDPR-modenhed i forhold til kriteriet var på niveau 2,7 (her gennemsnittet af enhedernes besvarelser).

20. Oplysningspligt

Kriteriet oplysningspligt afspejler et krav direkte efter GDPR, hvorefter borgerne skal orienteres skriftligt om behandlingsformål og behandlingshjemmel og hvis relevant om øvrige forhold i forbindelse med organisationens første indsamling persondata om borgerne. Efterlevelse af oplysningspligten i en organisation forudsætter, at der er etableret nedskrevet procedure, som sikrer overholdelse af oplysningspligten. I målingen af kriteriet blev der målt på, om der i enhederne er nedskrevet procedure for efterlevelse af oplysningspligten.

Kommunens GDPR-modenhed i forhold til kriteriet var på niveau 2,3 (her gennemsnit af enhedernes besvarelser).

21. Håndtering af registreredes (borgernes) rettigheder

Kriteriet håndtering af borgernes rettigheder afspejler et krav direkte efter GDPR, hvorefter organisationen rettidigt skal håndtere henvendelser fra borgere, som gør brug af deres rettigheder efter GDPR (f.eks. indsigtsanmodninger). Håndtering af borgernes henvendelser/rettigheder forudsætter også, at der er etableret nedskrevet procedure, som sikrer rettidig håndtering af henvendelser fra borgerne. I målingen på kriteriet blev der målt på, om der i enhederne er nedskrevet procedure for håndtering af henvendelser/anmodninger fra borger, som gør brug af deres rettigheder efter GDPR.

Kommunens GDPR-modenhed i forhold til kriteriet var på niveau 2,4 (her gennemsnit af enhedernes besvarelser).

22. Persondatasikkerhedsbrud

Kriteriet persondatasikkerhedsbrud afspejler et krav direkte efter GDPR, hvorefter

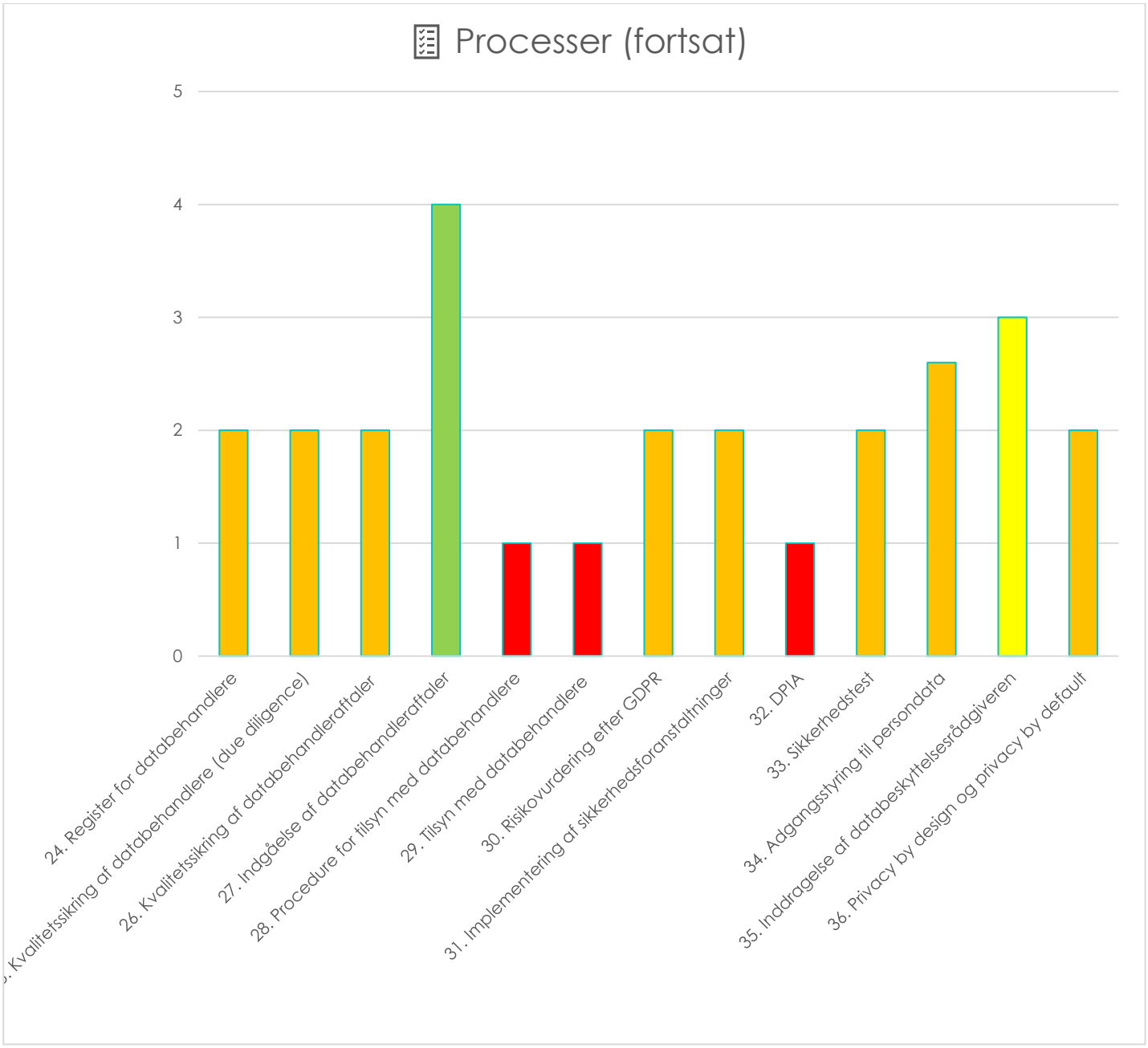
persondatasikkerhedsbrud skal registreres i organisationen og i nogle tilfælde anmeldes til Datatilsynet samt underrettes om til borgerne, hvis relevant. I målingen på kriteriet blev der målt på, om der i kommunen er nedskrevet procedure, som sikrer håndtering af persondatasikkerhedsbrud.

Kommunens GDPR-modenhed i forhold til kriteriet var på niveau 3.

23. Klager fra registrerede (borgerne)

Kriteriet klager fra borgerne afspejler ikke et krav direkte efter GDPR. I målingen af kriteriet blev der målt på, om der er en nedskrevet procedure for håndtering af klager fra borgerne, fordi nedskrevet procedure for håndtering af klager fra borgerne understøtter organisationen i at håndtere klager. Hvis klager ikke håndteres korrekt af organisationen, kan det føre til klagesager ved Datatilsynet.

Modenheden i kommunen i forhold til dette kriterium var på niveau 2.



24. Register for databehandlere

Register for databehandlere er et kriterium, som afspejler et krav direkte efter GDPR. Det følger af GDPR, at organisationen skal foretage tilsyn af databehandlere, hvilket forudsætter, at der er et overblik over alle databehandlere i organisationen. I målingen på kriteriet blev der målt på, om der i kommunen er etableret et centralt register for alle databehandlere i kommunen.

GDPR-modenhed i kommunen i forhold til kriteriet var på niveau 2.

25. Kvalitetssikring af databehandleren (due diligence)

Kriteriet kvalitetssikring af databehandleren (due diligence) afspejler et krav direkte efter GDPR, hvorefter organisationen 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 efterleve dette krav, skal organisationen foretage en kvalitetssikring (f.eks. gennemføre en questionnaire) af databehandleren, før der indgås en databehandleraftale med databehandleren. I målingen på kriteriet blev der målt på, om der i kommunen er etableret en nedskrevet procedure, som sikrer kvalitetssikring (due diligence) af databehandleren.

Kommunens GDPR-modenhed i forhold til dette kriterium var på niveau 2.

26. Kvalitetssikring af databehandleraftaler

Kriteriet om kvalitetssikring af databehandleraftaler afspejler et krav direkte efter GDPR, hvorefter databehandleres behandlinger af persondata for organisationen skal ske i henhold til en gyldig databehandleraftale i overensstemmelse med GDPR. I målingen på kriteriet er der målt på, om der foreligger en nedskrevet procedure for kvalitetssikring af databehandleraftaler i kommunen.

Kommunens GDPR-modenhed i forhold til dette kriterium var på niveau 2.

27. Indgåelse af databehandleraftaler

Kriteriet indgåelse af databehandleraftaler afspejler et krav direkte efter GDPR, hvorefter organisationen skal indgå databehandleraftaler med alle databehandlere, som behandler persondata på vegne af organisationen og efter organisationens instrukser.

Kommunens GDPR-modenhed i forhold til kriteriet var på niveau 4.

28. Procedure for tilsyn med databehandlere

Kriteriet afspejler et krav direkte efter GDPR, hvorefter organisationen skal være tilsyn af databehandleres overholdelse af betingelserne i indgåede databehandleraftaler, herunder implementering og opretholdelse af sikkerhedsforanstaltninger for beskyttelse af persondata. I målingen på kriteriet blev der målt på, om der foreligger nedskrevet procedure, som sikrer, at der foretages tilsyn af databehandlere i kommune.

Kommunens GDPR-modenhed i forhold til dette kriterium var på niveau 1.

29. Tilsyn med databehandlere

Det er et krav direkte efter GDPR, at kommunen gennemfører tilsyn med databehandlere. Tilsyn skal gennemføres på baggrund af en risikobaseret tilgang.

Kommunens GDPR-modenhed i forhold til kriteriet var på niveau 1.

Det skal bemærkes, at der er truffet beslutning i kommunen om at uddelegere gennemførelse af tilsyn med fælles databehandlere for kommuner i Den Storkøbenhavnske Digitaliseringsforening til en tilsynsfunktion, som er etableret i Den Storkøbenhavnske Digitaliseringsforening. Kommunen vil fortsat skulle gennemgå og forholde sig til tilsynsrapporter fra tilsynsfunktionen i Den Storkøbenhavnske Digitaliseringsforening, ligesom kommunen vil skulle gennemføre tilsyn med databehandlere, som ikke omfattes af tilsyn hos tilsynsfunktionen i Den Storkøbenhavnske Digitaliseringsforening.

30. Risikovurderinger efter GDPR

Kriteriet risikovurderinger efter GDPR afspejler et krav direkte efter GDPR, hvorefter organisationen i forhold til enhver behandling af persondata skal gennemføre risikovurderinger, som tager højde for de hensyn, som følger af GDPR. Det følger af ansvarlighedsprincippet, at organisationen skal kunne påvise, at der er gennemført risikovurderinger, som lever op til kravene efter GDPR. I målingen på kriteriet blev der målt på, om kommunen gennemfører dokumenterede risikovurderinger i overensstemmelse med GDPR.

GDPR-modenhed i kommunen i forhold til kriteriet var på niveau 2.

31. Implementering af sikkerhedsforanstaltninger

Kriteriet implementering af sikkerhedsforanstaltninger afspejler et krav direkte efter GDPR, hvorefter organisationen skal implementere passende sikkerhedsforanstaltninger (tekniske og organisatoriske) for at sikre et passende sikkerhedsniveau for persondata. Passende sikkerhedsforanstaltninger skal implementeres på baggrund af risikovurderinger efter GDPR.

GDPR-modenhed i kommunen i forhold til dette kriterium var på niveau 2.

32. DPIA (konsekvensanalyser)

Konsekvensanalyser er et kriterium, som afspejler et krav direkte efter GDPR. Konsekvensanalysere handler om at sikre beskyttelse af persondata og beskytte borgernes rettigheder i forhold til behandlinger, som sandsynligvis vil indebære høje risici for borgernes rettigheder og frihedsrettigheder.

Formålet med at gennemføre konsekvensanalyser er at reducere den høje risici, som en behandling måtte indebære. I målingen på kriteriet er der målt på, om der foreligger en nedskrevet procedure i kommunen, som sikrer en ensartet overvejelse af, om der skal udføres konsekvensanalyser i forhold til type af behandlinger, som kan indebære høje risici for borgernes rettigheder og frihedsrettigheder.

GDPR-modenheden i kommunen i forhold til kriteriet var på niveau 1.

33. Sikkerhedstest

Kriteriet sikkerhedstest afspejler et krav direkte efter GDPR, hvorefter der skal gennemføres sikkerhedstest, som sikrer løbende afprøvning og vurdering af implementerede sikkerhedsforanstaltningers effektivitet. I målingen på kriteriet blev der målt på, om der er etableret nedskrevet procedure, som sikrer, at der gennemføres sikkerhedstest.

GDPR-modenhed i kommunen i forhold til dette kriterium var på niveau 2.

34. Adgangsstyring til persondata

Adgangsstyring til persondata er et kriterium, som afspejler et krav direkte efter GDPR, hvorefter organisationens ledere og medarbejdere kun må få adgang til de persondata (følsomme persondata) og systemer (systemer indeholdende følsomme persondata), som er nødvendige for udførelse af deres arbejdsopgaver. I målingen på kriteriet blev der målt på, om der er etableret nedskrevet procedure for autorisation og tildeling af rettigheder, som sikrer adgangsstyring til persondata og systemer i organisationen.

GDPR-modenheden i kommunen i forhold til dette kriterium var på niveau 2,6 (her gennemsnit af enhedernes besvarelser).

35. Inddragelse af databeskyttelsesrådgiveren

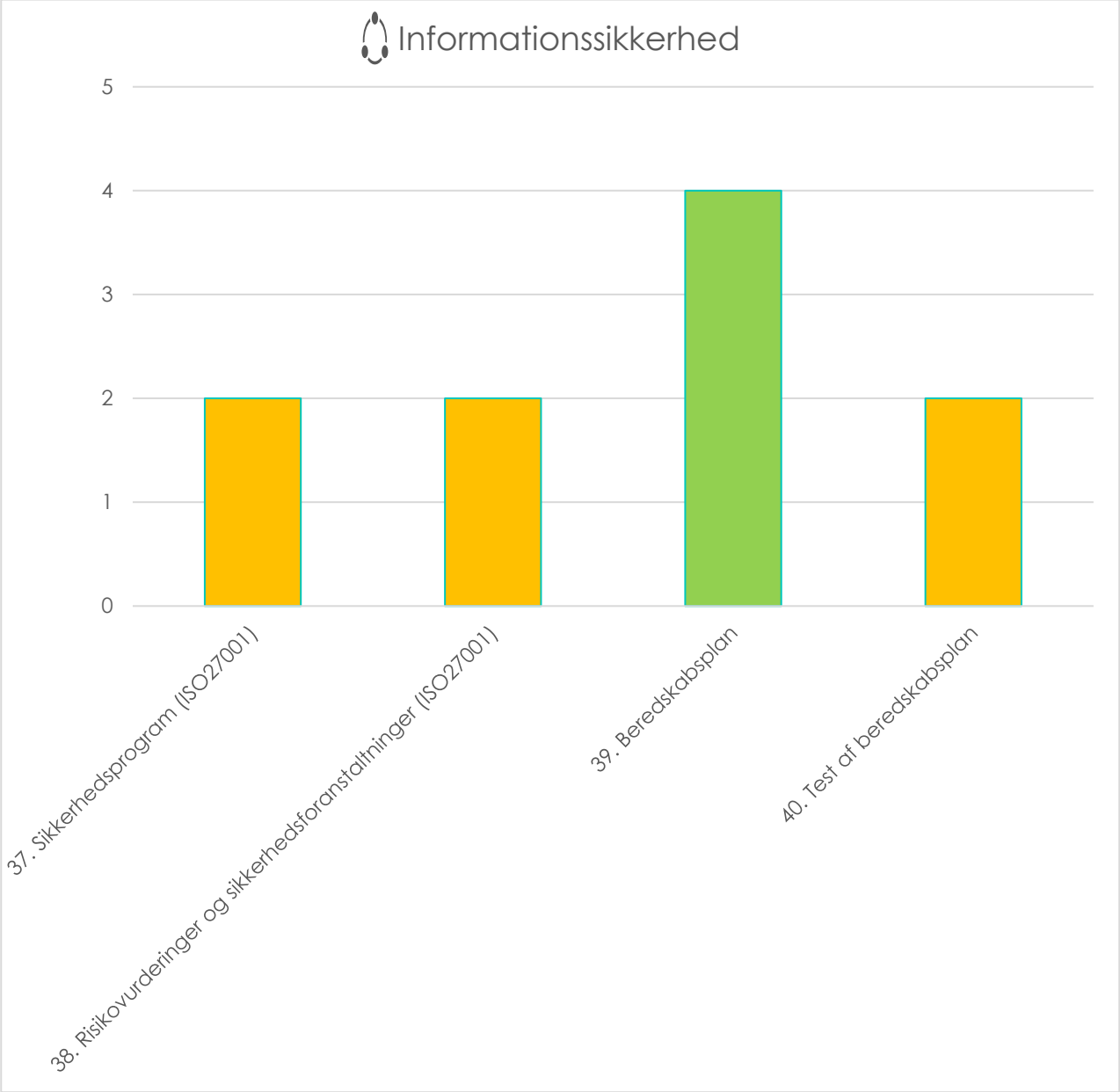
Inddragelse af databeskyttelsesrådgiveren er et kriterium, som afspejler et krav direkte efter GDPR, hvorefter organisationen skal inddrage databeskyttelsesrådgiveren rettidigt og i tilstrækkeligt omfang i forhold til alle spørgsmål vedrørende beskyttelse af persondata i organisationen. I målingen på kriteriet blev der målt på, om der er etableret en nedskrevet procedure i kommunen, som sikrer rettidig inddragelse af databeskyttelsesrådgiveren.

Kommunens GDPR-modenhed i forhold til kriteriet var på niveau 3.

36. Privacy by design og privacy by default

Privacy by design og privacy by default er et kriterium, som afspejler krav direkte efter GDPR, hvorefter nye it-systemer/løsninger i organisationen til behandling af persondata skal være designet/bygget således, at systemerne beskytter persondata og efterlever GDPR (privacy by design). Eksisterende systemer og processer i organisationen skal konfigureres/indstilles således, at persondata beskyttes og GDPR efterleves (privacy by default). I målingen på kriteriet blev der målt på, om der er en dokumenteret implementering af principper for privacy by design og privacy by default i forbindelse med implementering af nye systemer og løsninger i kommunen eller ved ændringer af eksisterende systemer.

Kommunens GDPR-modenhed i forhold til kriteriet var på niveau 2.



Introduktion til informationssikkerhed

Det følger af den fællesoffentlige digitaliseringsstrategi for 2016-2020, at kommuner 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.

37. Sikkerhedsprogram (ISO27001)

Kriteriet sikkerhedsprogram (ISO27001) afspejler det forhold, at implementering og drift af informationssikkerhed i en organisation forudsætter etablering af et sikkerhedsprogram (ISO27001).

Modenheden i kommunen i forhold til dette kriterium var på niveau 2.

Risikovurderinger og sikkerhedsforanstaltninger (ISO27001)

Kriteriet risikovurderinger og sikkerhedsforanstaltninger (ISO27001) afspejler et princip

efter ISO27001, hvorefter organisationen skal foretage risikovurdering og implementere sikkerhedsforanstaltninger for at bevare fortrolighed, integritet og tilgængelighed af informationsaktiver i organisationen.

Modenheden i kommunen i forhold til dette kriterium var på niveau 2.

38. Beredskabsplan

Kriteriet beredskabsplan afspejler et princip efter ISO27001, hvorefter der skal være en plan og procedure (beredskabsplan) i organisationen for videreførelse af kritiske forretningsprocesser i tilfælde af kritiske situationer (f.eks. ved omfattende hackerangreb).

Kommunens modenhed i forhold til kriteriet var på niveau 4.

39. Test af beredskabsplan

Test af beredskabsplan er et kriterium, som afspejler et princip efter ISO27001, hvorefter der skal være en procedure i organisationen for afprøvning og forbedring af beredskabsplan gennem regelmæssig træning, afprøvning og evaluering, hvormed der sikres et effektivt beredskab. Uden test af beredskabsplan ved organisationen ikke, om en beredskabsplan virker efter hensigten i tilfælde af kritiske situationer.

Kommunes modenhed i forhold til kriteriet var på niveau 2.

Bilag 2

Nøgletal fra kommunen om overholdelse af GDPR

Databeskyttelsesrådgiveren har indsamlet nøgletal fra kommunen om overholdelse af GDPR.

GDPR-ressourcer

Antal dedikerede GDPR-ressourcer	2018/2019
Årsværk til implementering og drift af GDPR	1

Kommunen har i perioden 2018-2019 haft et dedikeret årsværk (fordelt på mange personer) til implementering og drift af GDPR. Der er efter databeskyttelsesrådgiverens vurdering brug for at tilføre databeskyttelsesområdet flere ressourcer til implementering og drift af GDPR i kommunen. Med "dedikerede GDPR-ressourcer" menes medarbejdere, som har implementering eller drift af GDPR som fast arbejdsopgave, men implementering og drift af GDPR behøver ikke at være medarbejdernes eneste arbejdsopgaver.

Klager og anmodninger fra registrerede (borgerne)

Antal klager og anmodninger fra registrerede (borgerne)	2018/2019
Klager	3
Anmodninger:	
- Indsigt	9
- Indsigelser	1
- Berigtigelser	2
- Behandlingsophør	25
- Sletning	3
- Dataportabilitet	0
Anmodninger behandlet inden for lovfristen på 30 dage	38

Kommunen har modtaget i alt 40 anmodninger fra borgere, som har gjort brug af deres rettigheder efter GDPR. Hovedparten af anmodningerne omhandler behandlingsophør. Nøgletallene viser, at kommunen har håndteret langt hovedparten af anmodningerne fra borgerne inden for 30-dages fristen efter GDPR.

Nye it-løsninger og systemer

Antal nye it-systemer/løsninger	2018/2019
Anskaffelse af nye systemer til brug for behandling af persondata	3
Inddragelse af databeskyttelsesrådgiveren ved anskaffelse af nye systemer	0

Kommunen har efter det oplyste anskaffet 3 nye it-systemer/løsninger til brug for behandling af persondata i kommunen, men kommunen har ikke inddraget databeskyttelsesrådgiveren i forbindelse med anskaffelserne. Det er et krav efter GDPR, at kommunen skal inddrage databeskyttelsesrådgiveren i alle spørgsmål vedrørende beskyttelse af persondata. Det betyder bl.a., at databeskyttelsesrådgiveren i god tid og på et tilstrækkeligt grundlag skal inddrages ved anskaffelser af nye it-systemer/løsninger til brug for behandling af persondata i kommunen. Dette gælder navnlig i forhold til it-systemer/løsninger, som skal bruges til behandling af følsomme persondata.

Databeskyttelsesrådgiveren er heller ikke blevet inddraget af kommunen i anskaffelsesprocesser for nye it-systemer/løsninger til brug for behandling af persondata før offentliggørelse af udbudsmateriale, hvor kommunen i kravspecifikationer skal sikre, at systemerne er designet/bygget således, at systemerne beskytter persondata og efterlever GDPR (privacy by design)

DPIA (konsekvensanalyser)

Antal DPIA'er (konsekvensanalyser)	2018/2019
Gennemførte DPIA'er	0
Rådføring med databeskyttelsesrådgiveren ved gennemførelse af DPIA'er	0

Kommunen har endnu ikke gennemført konsekvensanalyser. Dette er et område – sammen med håndtering af databehandlere og risikostyring - hvor kommunen vil skulle sætte ind og prioritere for at efterleve GDPR, idet kommunen behandler følsomme persondata i stort omfang, og der må antages at være nye eller ændrede behandlinger, som indebærer høje risici for borgerne. Ligeledes bør kommunen - i takt med, at den anvender ny teknologi til behandling af persondata – sikre sig, at der gennemføres de fornødne konsekvensanalyser.

Persondatasikkerhedsbrud

Antal persondatasikkerheds-brud	2018/2019
Registrerede persondatasikkerhedsbrud	32
Brud anmeldt til Datatilsynet	22
Brud hvoraf der er sket underretning til registrerede (borgerne)	16
Anmeldelser til Datatilsynet inden for lovfristen på 72 timer	20

Kommunen har haft 32 persondatasikkerhedsbrud. Heraf er 22 persondatasikkerhedsbrud anmeldt til Datatilsynet. I langt hovedparten af persondatasikkerhedsbruddene, som er anmeldt til tilsynet, har kommunen overholdt 72-timers fristen efter GDPR. Tallene viser, at kommunen er opmærksom på at underrette borgerne om persondatasikkerhedsbrud, hvis dette vurderes relevant.

Intern kontrol

Antal intern kontrol (kommunens egne stikprøver)	2018/2019
Planlagte tilsyn	1
Gennemførte tilsyn	1

Tallene viser, at kommunen har gennemført en stikprøve af overholdelse af GDPR i kommunen, hvor kommunen har kontrolleret, om fagområderne har udfyldt dokumentation for behandlinger af persondata (såkaldt fortegnelse over behandlingsaktiviteter).

Stikprøver (monitorering) af overholdelse af GDPR i kommunen er et område, hvor kommunen vil skulle anvende ressourcer for at efterleve GDPR (gælder også i forhold til gennemførelse af sikkerhedstest for afprøvning og vurdering af sikkerhedsforanstaltningers effektivitet).

Tilsyn af Datatilsynet

Antal eksternt tilsyn (Datatilsynet)	2018/2019
Tilsyn	0
Emner for tilsyn:	-
Resultat:	-

Kommunen har efter det oplyste ikke haft sager ved Datatilsynet.

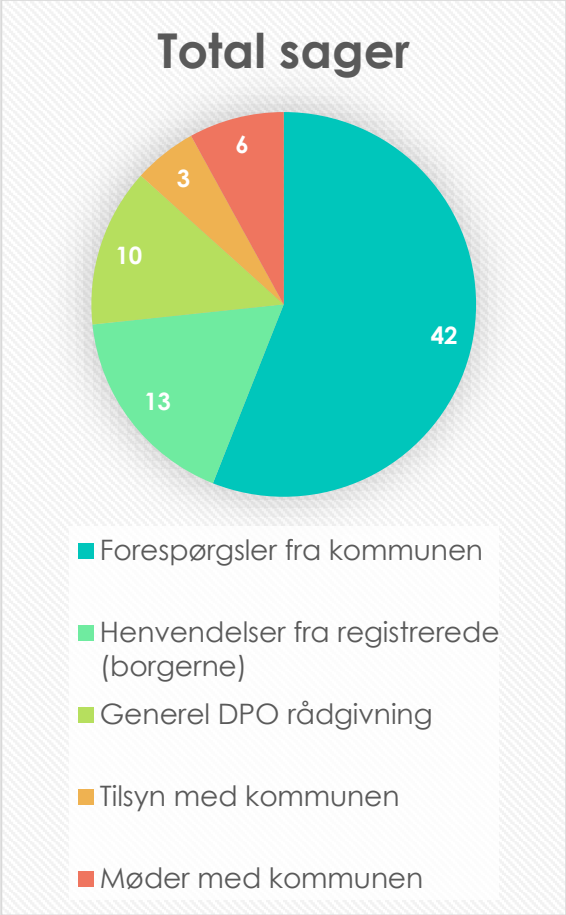
Opsamling

Nøgletallene fra kommunen om overholdelse af GDPR viser, at kommunen har håndteret langt hovedparten af anmodninger fra borgere (38 ud af 40) inden for 30-dages lovfristen efter GDPR. Nøgletallene viser desuden, at kommunen i forhold til langt hovedparten af persondatasikkerhedsbrud (20 ud af 22) som er anmeldt til Datatilsynet, har overholdt 72-timers fristen efter GDPR. Nøgletallene fra kommunen viser, at kommunen er opmærksom på at underrette de borgerne i tilfælde af persondatasikkerhedsbrud, hvis dette vurderes relevant.

Kommunen har efter det oplyste anskaffet 3 nye it-systemer, men kommunen har ikke inddraget databeskyttelsesrådgiveren i forbindelse med anskaffelserne – og dette gælder vel at mærke også i forhold til it-systemer/løsninger, som skal bruges til behandling af følsomme persondata i kommunen. Databeskyttelsesrådgiveren er heller ikke blevet inddraget i anskaffelsesprocesser for it-systemer/løsninger til brug for behandling af persondata før offentliggørelse af udbudsmateriale. Kommunen har kun i begrænset omfang (en gang) gennemført stikprøve af overholdelse af GDPR i kommunen, og kommunen har ikke gennemført konsekvensanalyser (DPIA).

Bilag 3

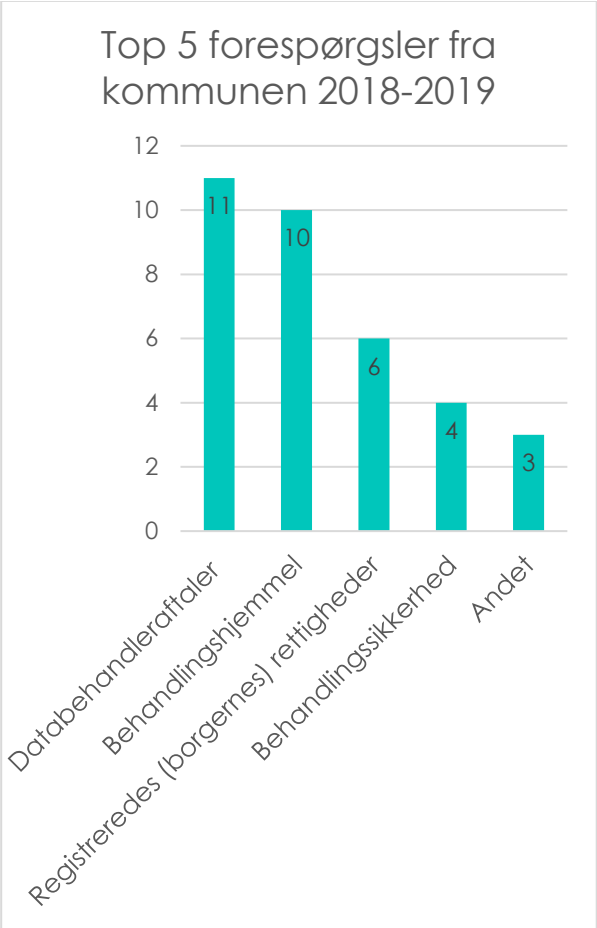
Sagsstatistik for databeskyttelsesrådgiverens arbejde



Antal sager

Databeskyttelsesrådgiveren har i perioden 25. maj 2018 til og med 31. december 2019 oprettet i alt 74 sager vedrørende kommunen, som er fordelt på sagskategorierne forespørgsler fra kommunen (42 sager), henvendelser fra borgere (13 sager), generel DPO-rådgivning (10 sager), tilsyn med kommunen (4 sager) og møder med kommunen (6 sager).

Forespørgsler fra kommunen



Top 1 forespørgsel fra kommunen omhandler databehandleraftaler, hvor databeskyttelsesrådgiveren har modtaget elleve forespørgsler. Forespørgslerne omfatter bl.a. spørgsmål om databehandlerkonstruktionsbegrebet og spørgsmål om indgåelse af databehandleraftaler med leverandører på forskellige områder.

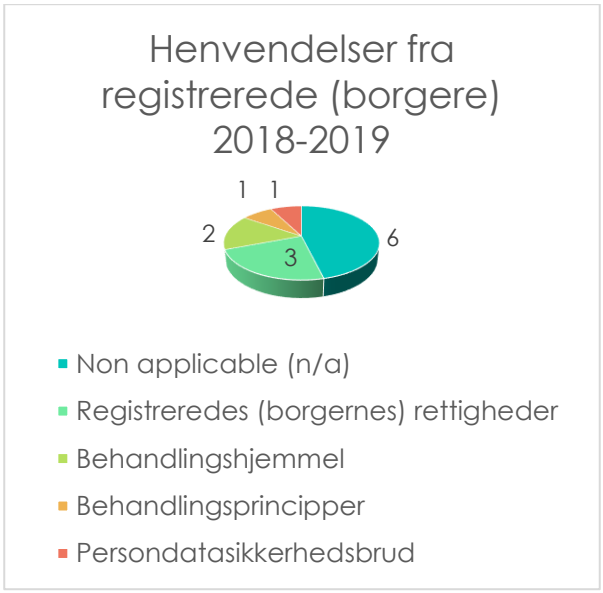
Top 2 forespørgsel omhandler behandlingshjemmel, hvor databeskyttelsesrådgiveren har modtaget ti forespørgsler fra kommunen. Forespørgslerne fra kommunen omfatter bl.a. spørgsmål om samtykke, behandling af persondata til statistik, brug af videooptagelser samt videregivelse af persondata.

Top 3 forespørgsel omhandler borgernes rettigheder efter GDPR. Databeskyttelsesrådgiveren har modtaget seks forespørgsler herom fra kommunen, som bl.a. omfatter spørgsmål om efterlevelse af oplysningspligten, undtagelser til pligten, herunder håndtering af indsigtsanmodninger.

Top 4 forespørgsel omhandler behandlingssikkerhed, hvor databeskyttelsesrådgiveren har modtaget fire forespørgsler fra kommunen. Forespørgslerne omfatter forskelligartede spørgsmål om sikkerhedsforanstaltninger.

Top 5 forespørgsel fra kommunen omfatter opsamlingskategorien "andet", hvor databeskyttelsesrådgiveren har modtaget tre forespørgsler, som vedrører spørgsmål om klassificering af persondata, samt roller og ansvar.

Henvendelser fra registrerede (borgerne)



Databeskyttelsesrådgiveren har modtaget 13 henvendelser fra borgere.

Seks henvendelser omhandlede spørgsmål til konkrete sager i kommunen eller spørgsmål til konkrete forhold i kommunen uden relevans for databeskyttelse (n/a). Tre henvendelser omhandlede anmodninger fra borgere, som gjorde brug af deres rettigheder efter GDPR (hhv. anmodninger om indsigt, berigtigelse og sletning) i forhold til de pågældende borgeres persondata i kommunen (registreredes rettigheder). Databeskyttelsesrådgiveren har videresendt disse henvendelser til behandling i kommunen.

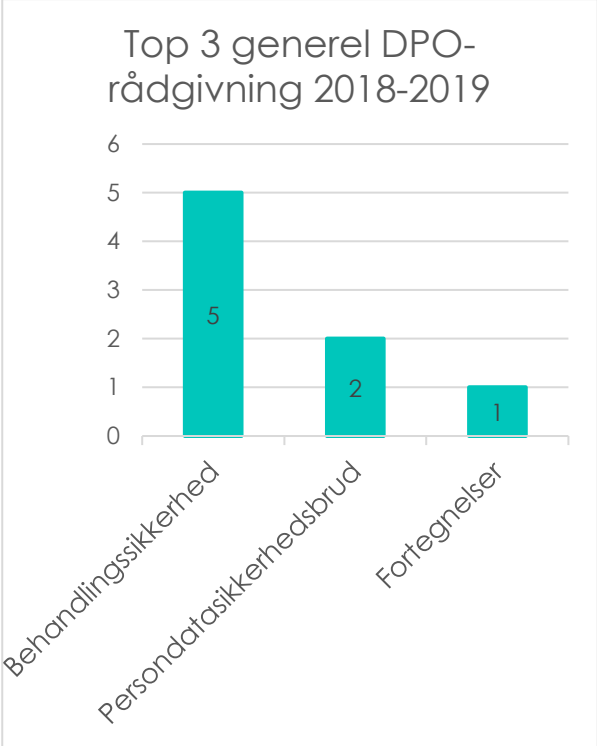
To henvendelser omhandlede spørgsmål om lovhjemmel i kommunen til behandling af persondata (behandlingshjemmel). Den ene sag omhandlede et generelt spørgsmål vedrørende hjemmel, hvor databeskyttelsesrådgiveren afsluttede sagen med generel vejledning til borgeren. Den anden sag omhandlede spørgsmål om Ishøj Svømmehals samtykkeerklæring til brug for indsamling og behandling af persondata om svømmehallens brugere. Databeskyttelsesrådgiveren foretog på baggrund af denne henvendelse et tilsyn med efterlevelse af GDPR-samtykkekrav i Ishøj Svømmehal (se afsnit om tilsyn med kommunen på side 25).

En anden henvendelse fra en borger omhandlede spørgsmål om opbevaring af persondata i Ishøj Svømmehal (behandlingsprincipper). Databeskyttelsesrådgiveren afsluttede denne sag med generel vejledning til borgeren.

En henvendelse omhandlede en borger, som underrettede databeskyttelsesrådgiveren om, at kommunen i forbindelse med en aktindsigt til vedkommende utilsigtet havde videregivet følsomme persondata om andre borgere (persondatasikkerhedsbrud). Databeskyttelsesrådgiveren vejledte generelt borgeren, og databeskyttelsesrådgiveren gav rådgivning samt anbefalinger til kommunen om håndtering af persondatasikkerhedsbruddet.

Generel rådgivning til kommunen

Sagskategorien generel DPO-rådgivning omfatter sager, hvor databeskyttelsesrådgiveren på eget initiativ rådgiver, giver anbefalinger eller holder oplæg for alle kommuner i Den Storkøbenhavnske Digitaliseringsforening.

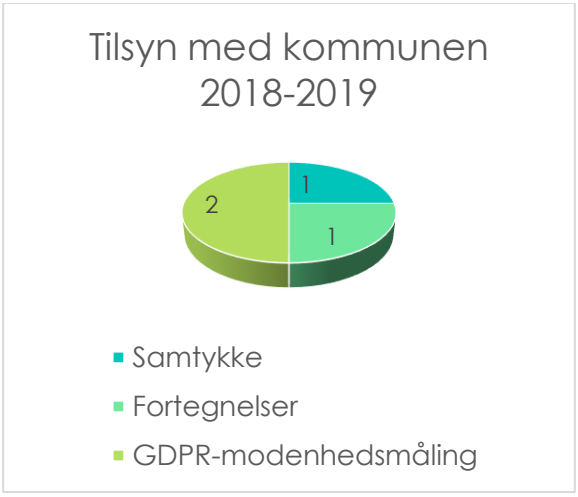


Top 1 generel DPO-rådgivning vedrører behandlingssikkerhed. Databeskyttelsesrådgiveren har i fem sager rådgivet kommunerne generelt om behandlingssikkerhed. Dette omfatter bl.a. anbefaling om foranstaltninger i tilfælde af hård-Brexit, anbefaling om sikring af tilsyn med underdatabehandlere samt anbefaling om kryptering af enheder, som indeholder følsomme persondata.

Top 2 generel DPO-rådgivning er om persondatasikkerhedsbrud, hvor databeskyttelsesrådgiveren i to sager har rådgivet og givet anbefalinger i anledning af sikkerhedsbrud, som har vedrørt alle kommuner i Den Storkøbenhavnske Digitaliseringsforening.

Databeskyttelsesrådgiveren har i en sag (top 3) rådgivet og anbefalet kommunerne i Den Storkøbenhavnske Digitaliseringsforening at sikre udspecificering af typer af følsomme persondata i kommunernes fortegnelser over behandlingsaktiviteter.

Tilsyn med kommunen



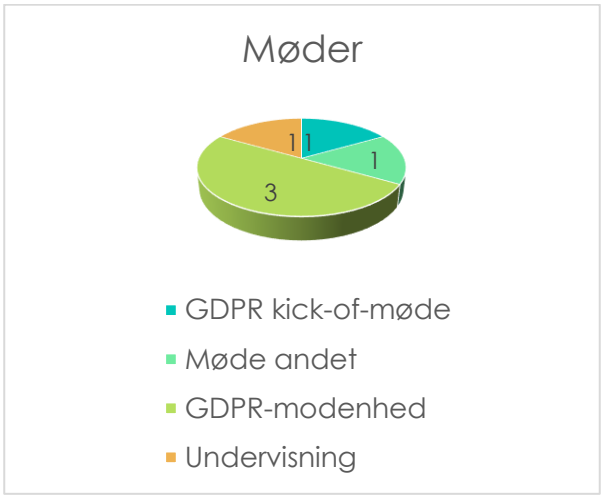
Databeskyttelsesrådgiveren har i medio 2018 foretaget et tilsyn med efterlevelse af GDPR-samtykkekrav i Ishøj Svømmehal i forhold til indsamling og behandling af persondata om svømmehallens brugere. Tilsynet identificerede mangler i svømmehallens samtykkeerklæring, som var utilstrækkelig til at indhente et gyldigt samtykke fra svømmehallens brugere til indsamling og behandling af deres persondata. Samtykkeerklæringen informerede ikke i tilstrækkelig grad svømmehallens brugerne om formålene med den behandling, som svømmehallen skulle bruge persondata til, ligesom brugerne ikke havde mulighed for at til- eller fravælge hvilke formål, brugerne reelt ønskede at give deres samtykke til. De af svømmehallen indhentede samtykker fra svømmehallens brugerne udgjorde således ikke et gyldigt behandlingsgrundlag for svømmehallens indsamling og behandling af persondata om brugerne. Databeskyttelsesrådgiveren har rådgivet og givet anbefalinger til kommunen omkring afhjælpning af manglerne og været i dialog med kommunen herom i ultimo 2018. Databeskyttelsesrådgiveren har i forbindelse med opfølgning i ultimo 2019 konstateret, at Ishøj Svømmehals samtykkeerklæring fortsat ikke i fuldt omfang efterlevede GDPR-samtykkekrav. Databeskyttelsesrådgiveren har underrettet kommunen herom.

Databeskyttelsesrådgiveren har i primo 2019 afsluttet et tilsyn med kommunens efterlevelse af GDPR-minimumskrav til fortegnelser over behandlingsaktiviteter. Tilsynet identificerede mangler i kommunens fortegnelser. Kommunen har oplyst, at

databeskyttelsesrådgiverens anbefalinger er indarbejdet i forbindelse med kommunens kortlægningsprojekt for kommunens fortegnelser over behandlingsaktiviteter.

Databeskyttelsesrådgiveren har endelig gennemført to tilsyn med kommunen i forbindelse med gennemførelse af GDPR-modenhedsmålinger i 2018 og 2019 (se bilag 1 for uddybning af GDPR-modenhedsmålingen fra 2019).

Møder med kommunen



Databeskyttelsesrådgiveren har deltaget på GDPR kick-of-møde med kommunens koncernledelse i forbindelse med tiltrædelsen som databeskyttelsesrådgiver (GDPR-kick-of-møde.

Databeskyttelsesrådgiveren har desuden deltaget på et andet ledelsesmøde i kommunen vedrørende GDPR-introduktion (møde andet).

Databeskyttelsesrådgiveren har herudover deltaget på to workshops i kommunen i forbindelse med gennemførelse af GDPR-modenhedsmålingen i 2019 samt på et møde med koncernledelsen vedrørende præsentation af resultater for GDPR-modenhedsmålingen i 2019 (GDPR-modenhed).

Databeskyttelsesrådgiveren har også deltaget på et møde i kommunen, hvor databeskyttelsesrådgiveren har undervist om risikovurdering og metode (undervisning).

Udover de ovenfor anførte mødesager har databeskyttelsesrådgiveren i de første seks måneder efter GDPR fik virkning gennemført regelmæssige GDPR-statusmøder med kommunen, og databeskyttelsesrådgiveren har desuden løbende holdt møder med kommunen, hvis det har været relevant i forbindelse med rådgivning. Databeskyttelsesrådgiveren har endelig deltaget regelmæssigt på GDPR-fortolkningsmøder for sikkerhedskoordinatorerne fra kommunerne i Den Storkøbenhavnske Digitaliseringsforening.

Leverancer til kommunen

Databeskyttelsesrådgiveren har udarbejdet en række vejledninger til kommunen om GDPR med henblik på at understøtte kommunen i forhold til efterlevelse af GDPR.

Vejledninger

- ✓ Oversigt over GDPR-krav og -aktiviteter
- ✓ Sikkerhedspolitikker
- ✓ Brug af kommunale aktiver
- ✓ Persondatapolitik
- ✓ Databehandlere
- ✓ Tilsyn med databehandlere
- ✓ Registreredes (borgernes) rettigheder
- ✓ Oplysningspligt
- ✓ Risikovurdering
- ✓ Adgangsstyring
- ✓ Roller og ansvar
- ✓ Inddragelse af databeskyttelsesrådgiveren
- ✓ Persondatasikkerhedsbrud
- ✓ Procedure for persondata-

Opsamling

Databeskyttelsesrådgiverens sager vedrørende kommunen viser, at kommunen har gjort brug af databeskyttelsesrådgiveren. Henvendelserne fra kommunen spænder over mange forskellige databeskyttelsesretlige spørgsmål, men de hyppigste henvendelser har omhandlet databehandleraftaler, behandlingshjemmel, borgernes rettigheder efter GDPR samt behandlingssikkerhed. To henvendelser fra borgere til databeskyttelsesrådgiveren har navnlig haft databeskyttelsesretlig relevans. Den ene henvendelse omhandlede underretning fra en borger til databeskyttelsesrådgiveren om, at kommunen i forbindelse med en aktindsigt til vedkommende utilsigtet havde videregivet følsomme persondata om andre borgere (persondatasikkerhedsbrud). Databeskyttelsesrådgiveren gav rådgivning og anbefalinger til kommunen om håndtering af persondatasikkerhedsbruddet. Den anden henvendelse omhandlede en henvendelse fra en borger vedrørende Ishøj Svømmehals brug af samtykke til indsamling og behandling af persondata om svømmehallens brugere. Databeskyttelsesrådgiveren foretog på baggrund af denne henvendelse et tilsyn med efterlevelse af GDPR-samtykkekrav i Ishøj Svømmehal. Tilsynet identificerede mangler i svømmehallens samtykkeerklæring, som var utilstrækkelig til at indhente et gyldigt samtykke fra svømmehallens brugere til indsamling og behandling af persondata om brugerne. De af svømmehallen indhentede samtykker fra svømmehallens brugere udgjorde således ikke et gyldigt behandlingsgrundlag for svømmehallens indsamling og behandling af persondata om brugerne. Databeskyttelsesrådgiverne har i forbindelse med opfølgning i ultimo 2019 konstateret, at svømmehallens samtykkeerklæring fortsat ikke i fuldt omfang efterlevede GDPR-samtykkekrav.