DATABESKYTTELSESRÅDGIVERENS ÅRSRAPPORT 2018-2019

Afsender:

Databeskyttelsesrådgiveren

Modtager:

Kommunalbestyrelsen i Rødovre 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. Reglerne gælder for Rødovre Kommune.

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

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 om konsekvensanalyser (herefter DPIA), at samarbejde med Datatilsynet og fungere som kontaktpunkt for Datatilsynet og for registrerede.

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 kr. 16 mio. til kommuner og andre offentlige myndigheder for manglende efterlevelse af GDPR.

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

Formålet med årsrapporten er at rapportere til kommunens øverste politiske ledelse om kommunens GPDR-modenhedsniveau og kommunens overholdelse af bestemmelserne i GDPR (herefter GDPR-compliance) samt at give anbefalinger for kommunens arbejde med databeskyttelse i 2020.

I rapportens ledelsesresumé er der en opsamling om kommunens GDPR-modenhedsniveau og GDPR-compliance i kommunen, en status for primo 2020 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 GDPR-compliance – overholdelse af GDPR-forordningens bestemmelser. Nøgletallene er indsamlet og opgjort i slutningen af 2019

Bilag 3 indeholder sagsstatistik for databeskyttelsesrådgiverens arbejde i perioden.

Daniel Soelberg Bach

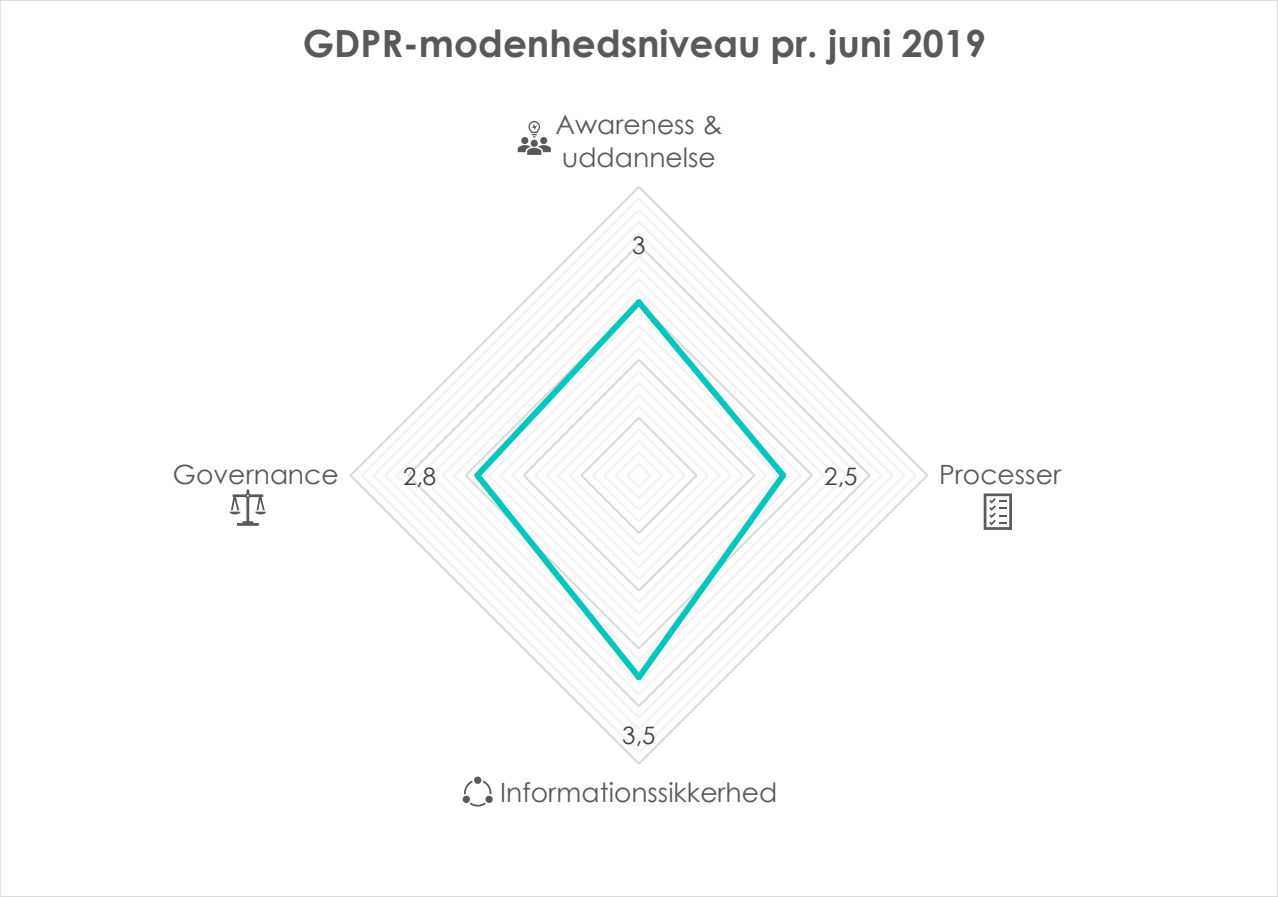
Databeskyttelsesrådgiver, Rødovre Kommune, 5. marts 2020.

Ledelsesresumé

GDPR-modenhedsniveau i kommunen

I juni 2019 gennemførte databeskyttelsesrådgiveren en GDPR-modenhedsmåling af Rødovre Kommune som led i databeskyttelsesrådgiverens lovpligtige opgave med at monitorere overholdelsen af de databeskyttelsesretlige regler i kommunen. Målingen omfattede 40 modenhedskriterier, som afspejler krav direkte efter GDPR eller forhold af betydning for GDPR. Målingen er baseret på en skala fra 1-5, hvor niveau 1 er lavest og 5 er højest (niveau 1-2 indikerer, at der ikke er GDPR-compliance, niveau 3 indikerer, at der er delvis GDPR-compliance. Niveau 4-5 indikerer, at der er GDPR-compliance). Resultaterne blev afrapporteret i en GDPR-modenhedsrapport til kommunens direktion i november 2019.

I den følgende model præsenteres resultaterne af målingen fordelt på fire hovedtemaer, hvorunder de 40 modenhedskriterier er placeret. Resultaterne fordelt på de enkelte modenhedskriterier foreligger i detaljeret form i bilag 1.



Kommunens gennemsnitlige GDPR-modenhedsniveau var 2,7 på tidspunktet for målingen.

Resultatet viser, at kommunens GDPR-modenhedsniveau var lavere end niveau 3 for mange modenhedskriterier, som afspejler opfyldelse af krav direkte efter GDPR. Dette indikerer, at kommunen på tidspunktet for målingen ikke var i GDPR-compliance i forhold til de pågældende krav. At ligge på det pågældende modenhedsniveau i forhold til de pågældende modenhedskriterier 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 overholdelse af de pågældende krav. 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 registreredes rettigheder (retten til databeskyttelse og retten til beskyttelse af privatlivets fred) ikke beskyttes.

På området for **governance** – ledelse og styring – viste målingen bl.a., at kommunen var godt på vej i forhold til kriterierne ledelsesmæssig understøttelse af GDPR-compliance, roller og ansvar samt kommunikation af databeskyttelsespolitikker. Niveauet var lavere for modenhedskriteriet monitorering af overholdelse af databeskyttelsespolitikker. I nogle fagområder var der et lavt modenhedsniveau for modenhedskriterierne kendskab til kommunens databeskyttelsespolitikker samt styring og rapportering omkring overholdelse af GDPR. Det laveste modenhedsniveau i fagområderne var for modenhedskriteriet ressourcer til arbejdet omkring overholdelse af GDPR.

På området for **awareness og uddannelse** viste målingen, at kommunen var godt på vej i forhold til både modenhedskriteriet awareness samt modenhedskriteriet uddannelse, selvom der i enkelte fagområder var et lavt modenhedsniveau for uddannelse.

På området for **processer** var det laveste gennemsnitsniveau for alle målte områder. Målingen viste bl.a., at der i fagområderne – med få positive udsving – var et lavt modenhedsniveau for modenhedskriterier, som afspejler grundlæggende behandlingsprincipper efter GDPR (dvs. indsamling af persondata til sagligt formål, datakvalitet, formålsbegrænsning og opbevaringsbegrænsning). Niveauet var også lavt for modenhedskriterier, som afspejler GDPR-krav om håndtering af databehandlere (dvs. register for databehandlere, kvalitetssikring af databehandlere (due diligence procedure for tilsyn med databehandlere samt gennemførelse af tilsyn med databehandlere), kvalitetssikring af databehandleraftaler, procedure for tilsyn af databehandleren samt tilsyn af databehandlere). Niveauet var endelig lavt for modenhedskriterier, som afspejler GDPR-krav om risikostyring (dvs. risikovurdering efter GDPR og implementering af passende sikkerhedsforanstaltninger samt sikkerhedstest af implementerede foranstaltningers effektivitet). I enkelte fagområder var der et lavt modenhedsniveau for modenhedskriteriet adgangsstyring til persondata.

På området for **informationssikkerhed** var det højeste gennemsnitlige GDPR-modenhedsniveau. Niveauet lå højt for alle modenhedskriterier (dvs. sikkerhedsprogram, risikovurdering og sikkerhedsforanstaltninger efter ISO27001, beredskabsplan samt test af beredskabsplan). Resultaterne for dette område viser, at kommunens indsats på området for informationssikkerhed har båret frugt.

GDPR-compliance

Nøgletallene fra kommunen om GDPR-compliance (se bilag 2) viser, at kommunen har håndteret alle anmodninger (20 ud af 20) fra registrerede, som har gjort brug af rettigheder efter GDPR, inden for lovfristen efter GDPR. Kommunen har desuden håndteret hovedparten af persondatasikkerhedsbrud (13 ud af 21), som er anmeldt til Datatilsynet, inden for lovfristen efter GDPR, og kommunen har været opmærksom på at underrette de registrerede, hvis relevant, ved persondatasikkerhedsbrud. En sag fra Datatilsynet, som er nævnt i bilag 2, hvor kommunen fik alvorlig kritik, viser, at der i forbindelse med et persondatasikkerhedsbrud i kommunen i et tilfælde uberettiget blev videregivet følsomme persondata til tredjemand.

Kommunen er generelt godt på vej i forhold til inddragelse af databeskyttelsesrådgiveren i anskaffelser af nye it-systemer/løsninger til brug for behandling af persondata, hvor kommunen har inddraget databeskyttelsesrådgiveren i 4 ud af 5 anskaffelser af it-systemer. Databeskyttelsesrådgiveren oplever endnu ikke at blive inddraget tidligt i processer for anskaffelse af it-systemer/løsninger før offentliggørelse af udbudsmateriale, hvor kommunen i kravspecifikationer skal tage højde for privacy by design (dvs. anskaffelser til brug for behandling af persondata skal fra start være designet således, at behandlingsprincipper efter GDPR kan efterleves og persondata beskyttes.

Kommunen har ikke foretaget stikprøver internt i kommunen (monitorering) af GDPR-compliance, hvilket er et krav efter GDPR. Kommunen har endnu ikke gennemført DPIA'er (data protection impact assessement), som er påkrævet efter GDPR i forhold til behandlinger, som sandsynligvis vil indebære en høj risiko for de registreredes rettigheder og frihedsrettigheder.

Der henvises i øvrigt til bilag 2 for en uddybning af nøgletallene.

Status primo 2020

Det er samlet set databeskyttelsesrådgiverens opfattelse, at der har været en positiv udvikling i kommunen siden GDPR-modenhedsmålingen blev foretaget i juni 2019. Databeskyttelsesrådgiveren lægger i den forbindelse vægt på, at kommunen har gennemført et stort kortlægningsprojekt af behandlingsaktiviteter, som kan anvendes som løftestang til at øge GDPR-modenheden og GDPR-compliance i kommunen, samt vægt på, at kommunen er i færd med at udarbejde en handleplan for, hvordan kommunen vil øge GDPR-modenheden.

Rødovre Kommune har i perioden 2018-2019 haft to dedikerede årsværk til arbejdet med implementering og drift af GDPR. Det er databeskyttelsesrådgiverens vurdering, at der er brug for flere ressourcer til implementering og drift af GDPR i kommunen henset til kommunens GDPR-modenhedsniveau fra målingen i juni 2019. Databeskyttelsesrådgiveren har noteret, at Rødovre Kommune har truffet beslutning om permanent tilførsel af yderligere 2 årsværk til arbejdet med implementering og drift af GDPR i kommunen. Det er databeskyttelsesrådgiverens vurdering, at tilførslen af de yderligere ressourcer til arbejdet med implementering og drift af GDPR er fornuftig og udgør et godt udgangspunkt for at øge GDPR-modenhedsniveauet i kommunen, 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, nedskrevne procedurer for sikring af håndtering af databehandlere, og med konkret håndtering af databehandlere og konkret risikostyring (løbende gennemførelse af risikovurderinger efter GDPR og implementering af sikkerhedsforanstaltninger på grundlag af GDPR-risikovurderinger). Dertil kommer, at kommunen også vil skulle monitorere overholdelse af databeskyttelsespolitikker/GDPR samt gennemføre DPIA'er, når det er påkrævet, for at være i GDPR-compliance.

Anbefalinger

Databeskyttelsesrådgiverens anbefalinger for kommunens arbejde med databeskyttelse i 2020 læner sig op ad anbefalingerne i GDPR-modenhedsrapporten til kommunens direktion. Databeskyttelsesrådgiveren anbefaler således kommunen at fokusere på at øge GDPR-modenhedsniveauet til minimum niveau 3 for så vidt angår modenhedskriterier, som afspejler krav direkte efter GDPR. Der er betydelig plads til at forbedre modenhedsniveauet i forhold til kriterier på området for processer, men der er også modenhedskriterier inden for området for governance (og awareness og uddannelse), hvor kommunen bør øge modenhedsniveauet.

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

- Kendskab til kommunens databeskyttelsespolitikker (i de fagområder, hvor kendskabet var på et lavt niveau)
- Monitorering af overholdelse af databeskyttelsespolitikker/GDPR
- Behandlingsprincipper efter GDPR, herunder navnlig opbevaringsbegrænsning i de fagområder, hvor opbevaringsbegrænsning var på et lavt niveau
- Håndtering af databehandlere (register for databehandlere, kvalitetssikring af databehandlere (due diligence), procedure for tilsyn med databehandlere samt gennemførelse af tilsyn med databehandlere)
- Risikostyring (risikovurdering efter GDPR og implementering af passende sikkerhedsforanstaltninger samt sikkerhedstest af implementerede foranstaltningers effektivitet)
- Adgangsstyring til personoplysninger (i de fagområder, hvor adgangsstyring var på et lavt niveau)

Databeskyttelsesrådgiveren anbefaler derudover kommunen at inddrage databeskyttelsesrådgiveren i design af kravspecifikationer før offentliggørelse af udbudsmateriale for hensyntagen til privacy by design i forbindelse med anskaffelse af nye it-systemer/løsninger til brug for behandling af persondata. Databeskyttelsesrådgiveren anbefaler endelig kommunen at fokusere på at gennemføre DPIA'er før behandling af persondata i nye systemer/løsninger, hvis behandlingen sandsynligvis vil indebære en høj risiko for de registreredes rettigheder og frihedsrettigheder, herunder sørge for at inddrage databeskyttelsesrådgiveren i tilfælde hvor der måtte være tvivl om, hvorvidt en DPIA 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/monitorere overholdelsen af de databeskyttelsesretlige regler i kommunen.

Formålet med at gennemføre en GDPR-modenhedsmåling er at måle compliancenieveauet 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.

Omfang

Der er gennemført en måling på baggrund af en række modenhedskriterier i Digitaliseringsafdelingen i Rødovre Kommune, som har ansvar for tværgående mål, rammer og foranstaltninger, som omfattes af GDPR. Og en måling på baggrund af andre modenhedskriterier i hver af Rødovre Kommunes nitten fagområder, som har ansvar for overholdelse af regler i GDPR.

Modenhedskriterier

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

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

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

Awareness og uddannelse

12. Awareness*
13. Uddannelse*

Processer

14. Fortegnelse*
15. Indsamling til sagligt formål*
16. Datakvalitet*
17. Formålsbegrænsning*
18. Opbevaringsbegrænsning*
19. Samtykke efter GDPR*
20. Oplysningspligt*
21. Håndtering af registreredes rettigheder*
22. Persondatasikkerhedsbrud*
23. Klager fra registrerede
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*
33. Sikkerhedstest*
34. Adgangsstyring til persondata*
35. Inddragelse af databeskyttelsesrådgiveren*
36. Privacy by design og privacy by default*

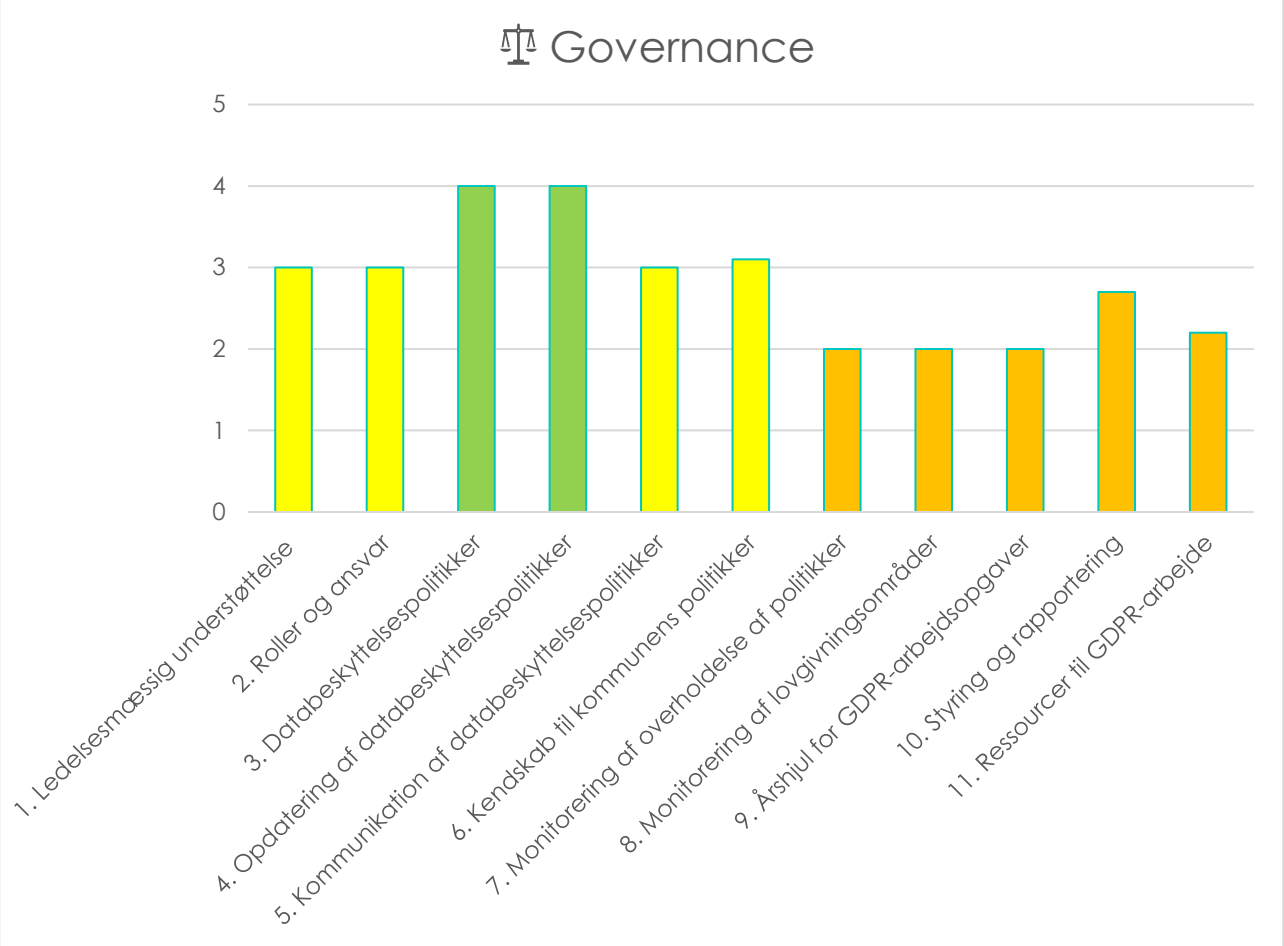
Informationssikkerhed

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

Skala

Niveau	Beskrivelse	Compliance
1	GDPR-compliance 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 der ikke er GDPR-compliance. Niveau 3 indikerer delvis GDPR-compliance. Modenhedsniveau 4-5 indikerer GDPR-compliance.
Terminologien "indikation" på ikke GDPR-compliance, "indikation" på delvis GDPR-compliance samt "indikation" på GDPR-compliance og 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 GDPR-compliance ved at kommunikere klart og tydeligt i kommunen om vigtigheden ved af overholde GDPR.

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

2. Roller og ansvar

Roller og ansvar er et kriterium, som afspejler krav direkte efter GDOR, hvorefter roller og ansvar for GDPR-compliance 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 4.

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 databeskyttelsespolitikker

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 3.

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 3,1 (her gennemsnit af fagområdernes 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 2.

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 2.

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

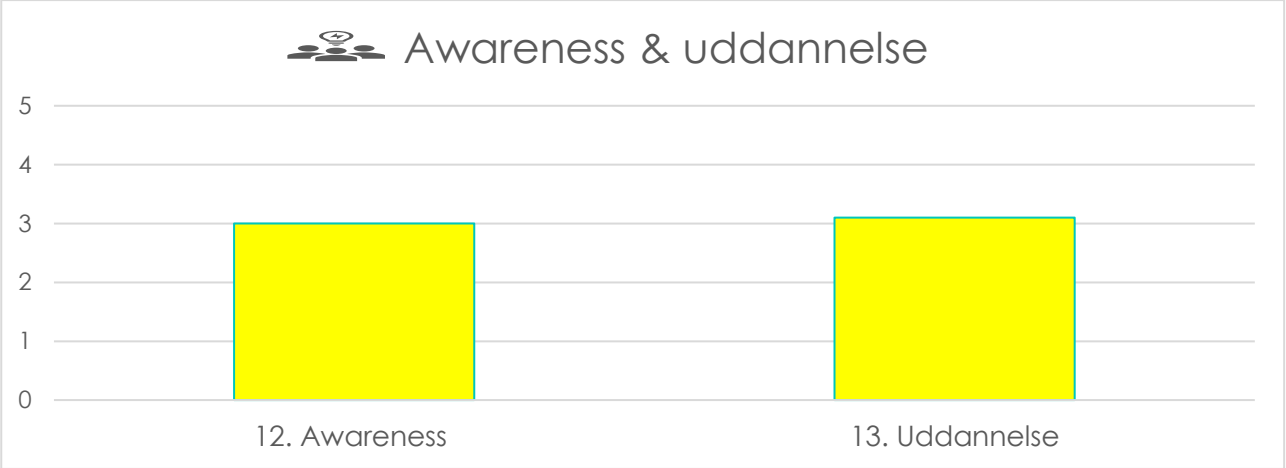
Styring og rapportering er et kriterium, som ikke afspejler et krav direkte efter GDPR. Der er målt på kriteriet, fordi kriteriet har betydning for implementering og drift af GDPR i fagområderne i organisationen

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

11. Ressourcer til GDPR-arbejde

Ressourcer til GDPR-arbejde er er ikke et kriterium, som afspejler et krav direkte efter GDPR, men tilstrækkelige ressourcer (f.eks. medarbejdere, tekniske løsninger og konsulenter) i fagområderne 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 2,2 (her gennemsnit af fagområdernes besvarelser).



12. Awareness

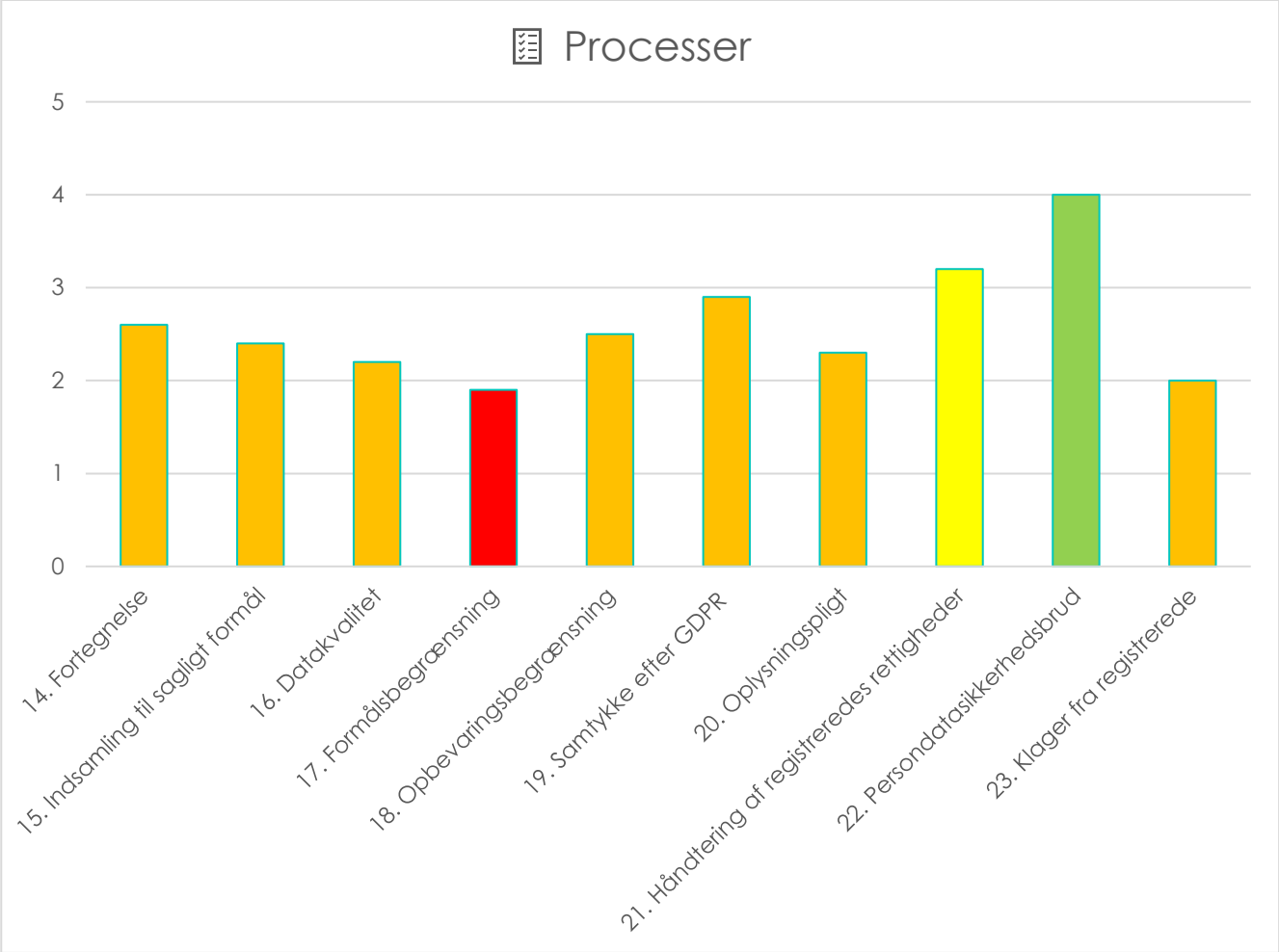
Kriteriet awareness afspejler et krav direkte efter GDPR, hvorefter ledere og medarbejdere i organisationen løbende skal informeres om beskyttelse af persondata for at skabe opmærksomhed og varsomhed omkring beskyttelse af persondata i organisationen.

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

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 3,1 (her gennemsnit af fagområdernes besvarelser).



14. Fortegnelse

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

Kommunens GDPR-modenhed i forhold til kriteriet var på niveau 2,6 (her gennemsnit af fagområdernes 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 fagområderne 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 fagområdernes 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 fagområdernes 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 1,9 (her gennemsnit af fagområdernes 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 p niveau 2,5 (her gennemsnittet af fagområdernes 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 de registrerede. 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 2,9 (her gennemsnittet af fagområdernes besvarelser).

20. Oplysningspligt

Kriteriet oplysningspligt afspejler et krav direkte efter GDPR, hvorefter de registrerede skal orienteres skriftligt om behandlingsformål og behandlingshjemmel og øvrige forhold i forbindelse med organisationens første indsamling persondata om de registrerede. 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 fagområderne er nedskrevet procedure for efterlevelse af oplysningspligten.

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

21. Håndtering af registreredes rettigheder

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

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

22. Persondatasikkerhedsbrud

Kriteriet persondatasikkerhedsbrud afspejler et krav direkte efter GDPR, hvorefter

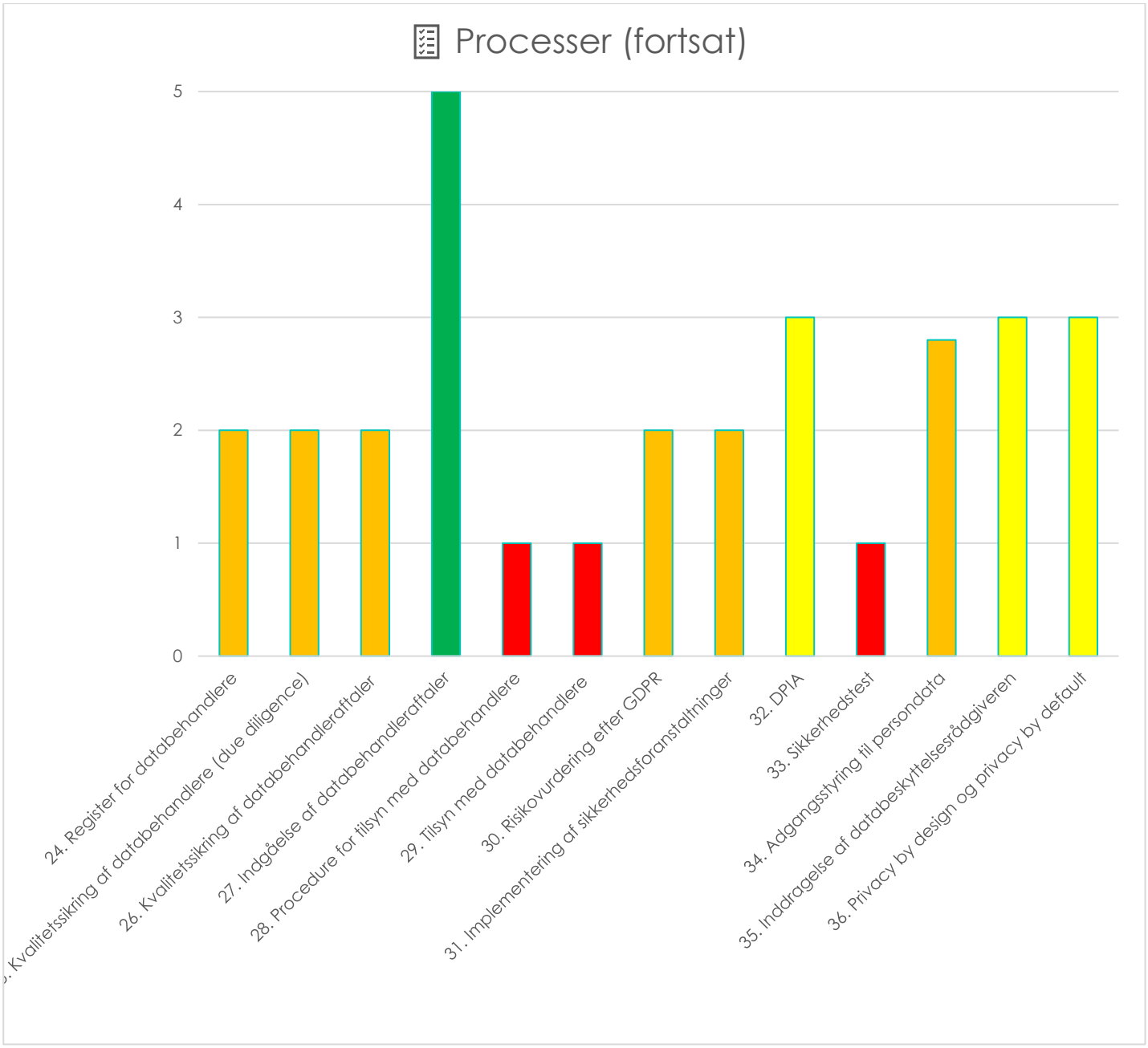
persondatasikkerhedsbrud skal registreres i organisationen og i nogle tilfælde anmeldes til Datatilsynet samt underrettes om til de registrerede. I målingen på kriteriet blev der målt på, om der i kommunen er nedskrevet procedure, som sikrer håndtering af persondatasikkerhedsbrud.

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

23. Klager fra registrerede

Kriteriet klager fra registrerede afspejler ikke et krav direkte efter GDPR. Der er målt på Kriteriet, om der er en nedskrevet procedure for håndtering af klager fra registrerede, fordi nedskrevet procedure for håndtering af klager fra registrerede understøtter organisationen i at håndtere klager, som hvis de ikke håndteres korrekt af organisationen, kan 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 5.

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 2.

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 dette kriterium var på niveau 1.

Det skal bemærkes, at der er truffet beslutning i Rødovre Kommune 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 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

DPIA er et kriterium, som afspejler et krav direkte efter GDPR. DPIA handler om at sikre beskyttelse af persondata og beskytte de registreredes rettigheder i forhold til behandlinger, som sandsynligvis vil indebære en høj risiko for de registreredes rettigheder og frihedsrettigheder. Formålet med at

gennemføre DPIA'en er at reducere den høje risiko, 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 en DPIA i forhold til type af behandlinger, som kan indebære en høj risiko for de registreredes rettigheder og frihedsrettigheder.

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

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 1.

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 2,8 (her gennemsnit af fagområdernes besvarelser).

35. Inddragelse af databeskyttelsesrådgiveren

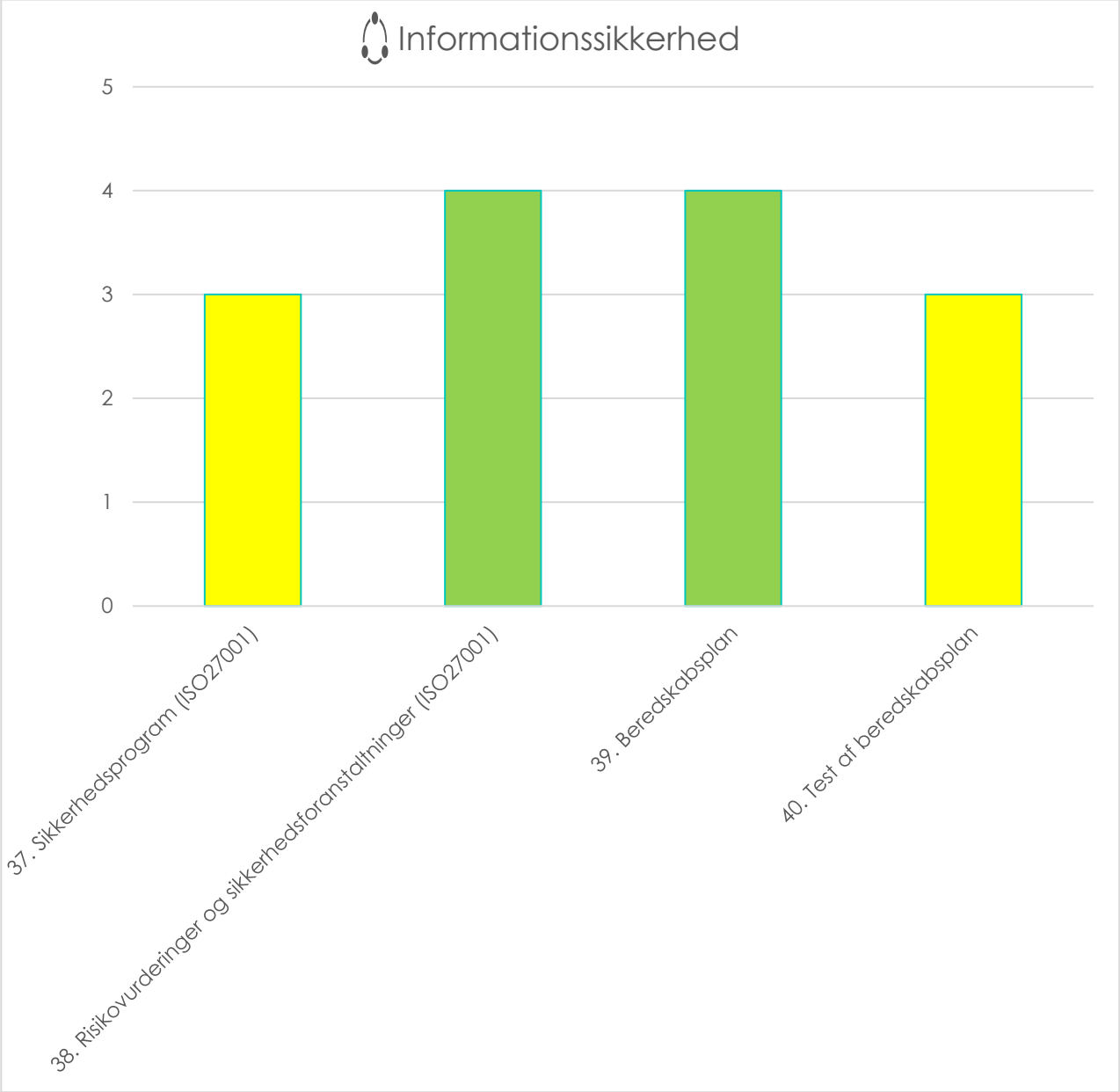
Inddragelse af databeskyttelsesrådgiveren er et kriterium, som afspejler et krav direkte efter GDPR, hvorefter organisationen skal inddrage databeskyttelsesrådgiveren rettidigt og i tilstrækkeligt omfang i forhold til alle spørgsmål vedrørende beskyttelse af persondata i organisationen. I målingen på 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 således, at behandlingsprincipper efterleves og persondata beskyttes (privacy by design). Eksisterende systemer/løsninger i organisationen skal konfigureres/indstilles således, at behandlingsprincipperne efterleves og persondata beskyttes (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 3.



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 3.

38. 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 4.

39. 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.

40. 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 3.

Bilag 2

Nøgletal fra kommunen om GDPR-compliance

Databeskyttelsesrådgiveren har indsamlet nøgletal fra kommunen om GDPR-compliance.

GDPR-ressourcer

Antal dedikerede GDPR-ressourcer	2018/2019
Årsværk til implementering og drift af GDPR	2

Kommunen har i perioden 2018-2019 haft 2 dedikerede årsværk til implementering og drift af GDPR. Det er databeskyttelsesrådgiverens vurdering, at der er brug for flere ressourcer end ressourcerne i kommunen i perioden 2018-2019 for at øge GPDR-modenhedsniveauet i kommunen fremadrettet.

Klager og anmodninger fra registrerede

Antal klager og anmodninger fra registrerede	2018/2019
Klager	3
Anmodninger:	
- Indsigt	16
- Indsigelser	1
- Berigtigelser	1
- Behandlingsophør	0
- Sletning	2
- Dataportabilitet	0
Anmodninger behandlet inden for lovfristen på 30 dage	20

Tallene viser, at registrerede har klaget til kommunen over behandlingen af persondata i kommunen, herunder at registrerede har henvendt sig til kommunen vedrørende anmodninger om brug af rettigheder efter GDPR. Rødovre Kommune har håndteret alle henvendelserne fra de registrerede vedrørende anmodninger om brug af rettigheder inden for 30-dages fristen efter GDPR, hvilket viser, at kommunens implementering af nedskrevet procedure for håndtering af henvendelser fra registrerede vedrørende anmodninger om brug af rettigheder efter GDPR fungerer.

Nye it-løsninger og systemer

Antal nye it-systemer/løsninger	2018/2019
Anskaffelse af nye systemer til brug for behandling af persondata	5
Inddragelse af databeskyttelsesrådgiveren ved anskaffelse af nye systemer	4

Kommunen har efter det oplyste anskaffet 5 nye it-systemer/løsninger til brug for behandling af persondata i kommunen, hvoraf databeskyttelsesrådgiveren er blevet inddraget i 4 af anskaffelserne. Det viser, at kommunens nedskrevne procedure for inddragelse af databeskyttelsesrådgiveren er begyndt at fungere. Databeskyttelsesrådgiveren oplever dog ikke at blive inddraget tidligt i anskaffelsesprocesser før offentliggørelse af udbudsmateriale, hvor kommunen i kravspecifikationer skal tage højde for privacy by design.

DPIA

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

Kommunen har endnu ikke gennemført DPIA'er. Dette er et område – sammen med håndtering af databehandlere og risikostyring - hvor kommunen vil skulle sætte ind og prioritere for at være i GDPR-compliance, idet kommunen behandler følsomme persondata i stort omfang, og der må antages at være behandlinger, som indebærer en høj risiko for de registrerede. Ligeledes bør kommunen - i takt med, at den anvender ny teknologi til behandling af persondata – sikre sig, at der gennemføres de fornødne DPIA´er.

Persondatasikkerhedsbrud

Antal persondatasikkerheds-brud	2018/2019
Registrerede persondatasik-kerhedsbrud	45
Brud anmeldt til Datatilsynet	21
Brud hvoraf der er sket under-retning til registrerede	12
Anmeldelser til Datatilsynet in-den for lovfristen på 72 timer	13

Rødovre Kommune har haft relativt mange persondatasikkerhedsbrud, men tallene vi-ser, at kommunen har håndteret hovedpar-ten af persondatasikkerhedsbrud, som skal anmeldes til Datatilsynet, inden for lovfristen på 72 timer, og kommunen har været op-mærksom på at underrette registrerede om persondatasikkerhedsbrud, hvis relevant. Tallene viser, at Rødovre Kommunes imple-mentering af nedskrevet procedure for per-sondatasikkerhedsbrud fungerer.

Intern kontrol

Antal intern kontrol (kommu-nens egne stikprøver)	2018/2019
Planlagte tilsyn	0
Gennemførte tilsyn	0

Tallene viser, at Rødovre Kommune endnu ikke er kommet i gang med at gennemføre stikprøver i kommunen i forhold til overhol-delse af databeskyttelsespolitikker/GDPR. Det er et område, hvor kommunen vil skulle anvende ressourcer for at være i GDPR-compliance (gælder også i forhold til gen-nemførelse af sikkerhedstest for afprøvning og vurdering af sikkerhedsforanstaltningers effektivitet).

Tilsyn af Datatilsynet

Antal eksternt tilsyn (Datatilsy-net)	2018/2019
Tilsyn	2
Emner for tilsyn 1:	
Indsamling af reference/vide-regivelse af oplysninger uden skriftligt samtykke	
Resultat:	
Sag henlagt (ingen kritik)	
Emne for tilsyn 2:	
Uberettiget videregivelse af persondata til tredjemand	
Resultat:	
Alvorlig kritik	

Rødovre Kommune har haft to sager ved Datatilsynet. I den ene sag blev databeskyt-telsesrådgiveren inddraget af kommunen forbindelse med udarbejdelse af høringssvar til Datatilsynet. Denne sag blev henlagt af Datatilsynet uden kritik, idet tilsynet ikke fandt, at den pågældende behandling havde været omfattet af GDPR. I den an-den sag, som omhandlede et persondata-sikkerhedsbrud i kommunen, udtalte Datatil-synet alvorlig kritik af kommunen, fordi kom-munen utilsigtet havde videregivet føl-somme persondata om en registreret til en tredjemand. Databeskyttelsesrådgiveren blev først inddraget af kommunen i forhold til den pågældende sag ved tilsynet efter, at Datatilsynet havde udtalt alvorlig kritik, og den registrerede havde sagsøgt kommunen ved domstolene. Den sene inddragelse af databeskyttelsesrådgiveren kan skyldes, at Datatilsynet ikke anvendte databeskyttel-sesrådgiveren som kontaktled i indgangen til kommunen, men under alle omstændighe-der bør kommunen inddrage databeskyttel-sesrådgiveren i verserende sager vedrø-rende kommunen ved Datatilsynet.

Begge sager har til fælles, at de udspringer af henvendelser fra registrerede, som har klaget over behandling af persondata i Rød-ovre Kommune. Sagen, hvor kommunen fik alvorlig kritik af tilsynet, viser, at kommunen i nogle tilfælde kan risikere erstatningssøgs-mål ved manglende efterlevelse af GDPR.

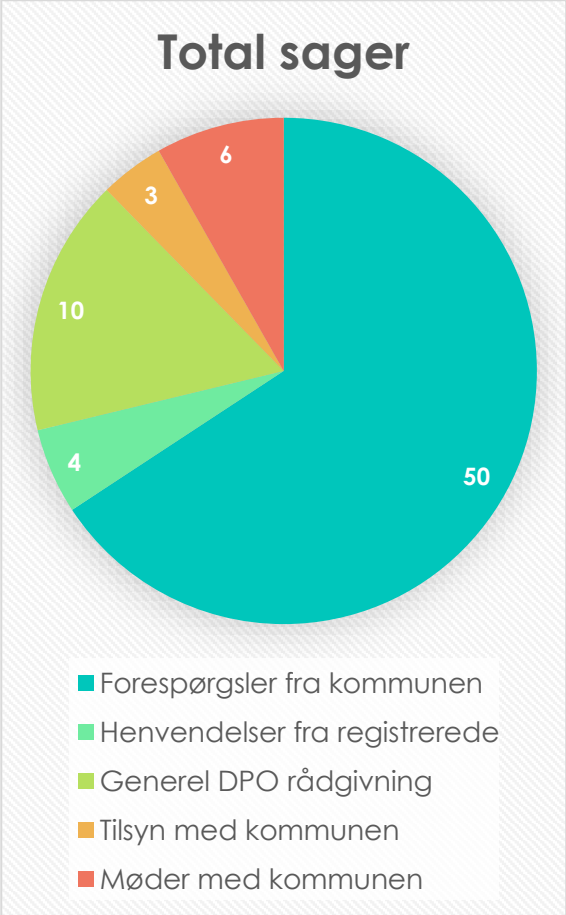
Opsamling

Nøgletallene fra kommunen om GDPR-com-pliance viser at kommunen har håndteret samtlige henvendelser fra registrerede in-den for lovfristen efter GDPR, herunder at kommunen har håndteret hovedparten af persondatasikkerhedsbrud, som skal anmel-des til Datatilsynet, inden for lovfristen efter GDPR. Kommunen er godt på vej i forhold til inddragelse af databeskyttelsesrådgiveren i anskaffelser af nye it-systemer/løsninger, men databeskyttelsesrådgiveren oplever ikke at blive inddraget tidligt i

anskaffelsesprocesser før offentliggørelse af udbudsmateriale. Kommunen har fået alvorlig kritik af Datatilsynet i en sag om uberettiget videregivelse af persondata til tredjemand. Rødovre Kommune har ikke gennemført DPIA'er og ikke foretaget stikprøver internt i kommunen af GDPR-compliance.

Bilag 3

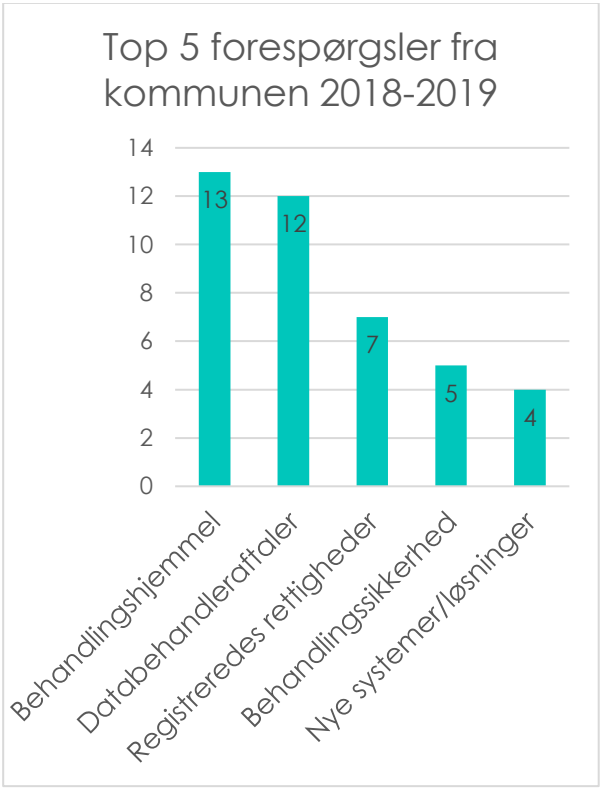
Sagsstatistik for databeskyttelsesrådgiverens arbejde



Antal sager

Databeskyttelsesrådgiveren har i perioden 25. maj 2018 til og med 31. december 2019 oprettet i alt 73 sager om Rødovre Kommune, som er fordelt på sagskategorierne forespørgsler fra kommunen (50 sager), henvendelser fra registrerede (4 sager), generel DPO-rådgivning (10 sager), tilsyn med kommunen (3 sager) og møder med kommunen (6 sager).

Forespørgsler fra kommunen



Top 1 forespørgsel fra kommunen omhandler behandlingshjemmel, hvor databeskyttelsesrådgiveren har modtaget tretten forespørgsler fra kommunen. Forespørgslerne fra kommunen omfatter bl.a. spørgsmål om samtykke, samkøring af persondata, indsamling og videregivelse af persondata.

Top 2 forespørgsel vedrører databehandleraftaler, hvor databeskyttelsesrådgiveren har modtaget tolv forespørgsler fra kommunen. Forespørgslerne omfatter bl.a. spørgsmål om databehandlerkonstruktionsbegrebet og spørgsmål om indgåelse af databehandleraftaler med leverandører på forskellige områder.

Top 3 forespørgsel vedrører registreredes rettigheder. Databeskyttelsesrådgiveren har modtaget syv forespørgsler fra kommunen vedrørende registreredes rettigheder. Kommunens forespørgsler omfatter bl.a. spørgsmål om behandling af konkrete indsigtsanmodninger og spørgsmål om overholdelse af oplysningspligten i forskellige sammenhænge.

Top 4 forespørgsel er om behandlingssikkerhed. Databeskyttelsesrådgiveren har modtaget fem forespørgsler herom fra

kommunen. Spørgsmålene fra kommunen vedrørende behandlingssikkerhed omfatter bl.a. sikker kommunikation, behandling i cloud og sikkerhedsforanstaltninger.

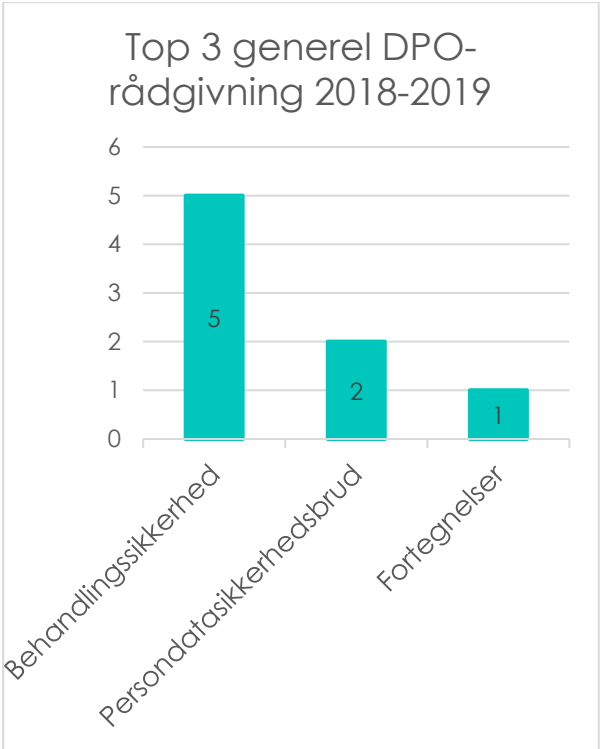
Top 5 forespørgsel omhandler nye systemer/løsninger. Databeskyttelsesrådgiveren har modtaget fire forespørgsler fra kommunen om inddragelse af databeskyttelsesrådgiveren i forbindelse med anskaffelse af nye systemer/løsninger til brug for behandling af persondata.

Henvendelser fra registrerede

Henvendelserne fra registrerede til databeskyttelsesrådgiveren vedrører relevante forhold i form af persondatasikkerhedsbrud, behandlingssikkerhed og behandlingshjemmel. Databeskyttelsesrådgiveren har vejledt de registrerede i det omfang, det har været relevant, og databeskyttelsesrådgiveren har været i dialog med kommunen og ydet rådgivning og givet anbefalinger omkring håndtering af henvendelserne.

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.

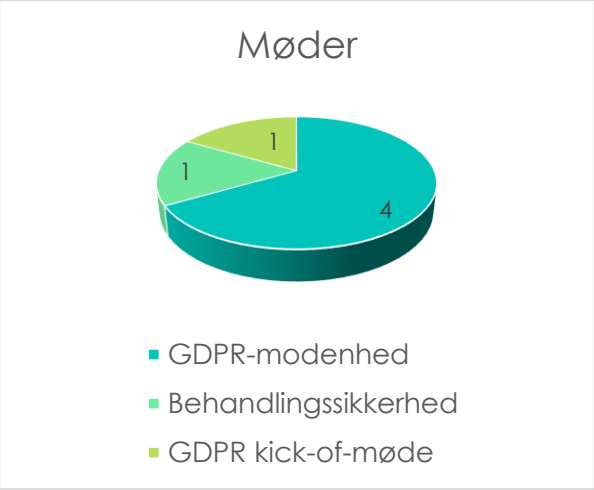
Databeskyttelsesrådgiveren har i en sag (top 3) rådgivet og anbefalet kommunerne i Den Storkøbenhavnske Digitaliseringsforening at sikre specificering af typer af følsomme persondata i kommunernes fortegnelser over behandlingsaktiviteter.

Tilsyn med kommunen

Databeskyttelsesrådgiveren har udført et tilsyn med kommunens efterlevelse af GDPR-minimumskrav til fortegnelser over behandlingsaktiviteter. Tilsynet identificerede mangler i kommunens fortegnelser, som kommunen efterfølgende har afhjulpet.

Databeskyttelsesrådgiveren har desuden gennemført to tilsyn med kommunen ved gennemførelse af GDPR-modenhedsmålinger i 2018 og 2019.

Møder med kommunen



Databeskyttelsesrådgiveren har deltaget på GDPR kick-of-møde med kommunen i forbindelse med tiltrædelsen som databeskyttelsesrådgiver for kommunen. Databeskyttelsesrådgiveren har deltaget på fire møder om GDPR-modenhed med kommunen. To af disse møder omfatter gennemførelse af workshop i kommunen i forbindelse med GDPR-modenhedsmålingen i 2019. To af møderne omfatter præsentation af resultater for GDPR-modenhedsmålinger i 2018 og 2019. Databeskyttelsesrådgiveren har desuden deltaget på et møde i kommunen for drøftelse af risikovurderinger.

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 holdt yderligere 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 GDPR-compliance.

Vejledninger

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

Opsamling

Databeskyttelsesrådgiverens sager om kommunen viser, at kommunen har gjort brug af databeskyttelsesrådgiveren. Henvendelserne fra kommunen spænder over mange forskellige databeskyttelsesretlige spørgsmål, men de hyppigste henvendelser har omhandlet spørgsmål om behandlingshjemmel, databehandleraftaler og registreredes rettigheder. Databeskyttelsesrådgiveren har modtaget få henvendelser fra registrerede, som har haft spørgsmål til behandling af persondata i kommunen, men henvendelser fra de registrerede har vedrørt relevante databeskyttelsesretlige spørgsmål, som databeskyttelsesrådgiveren har været i dialog om med kommunen. Sagerne, hvor databeskyttelsesrådgiveren af egen drift rådgiver og giver anbefalinger til kommunen, har omhandlet fortrinsvis spørgsmål om behandlingssikkerhed og persondatasikkerhedsbrud.