DATABESKYTTELSESRÅDGIVERENS ÅRSRAPPORT 2021

,

Afsender:

Andreas Drægert

Modtager:

Kommunalbestyrelsen i Rødovre Kommune

Indhold

Årsrapport 2021

I 2021 er der igen sket meget på databeskyttelsesområdet.

Kommunen lægger fortsat en stor arbejdsindsats i implementeringen af databeskyttelsesforordningens regler (herefter GDPR) samt i de tilhørende driftsopgaver.

I Rødovre Kommune har DPO'en rådgivet og vejledt kommunen ved forespørgsler. Endvidere har DPO'en ført tilsyn med kommunen ved at udføre audit på, om kommunen efterlever reglerne for tv-overvågning. Derudover har DPO´en gennemført den årlige GDPR-modenhedsmåling, som måler på kommunens niveau og forudsætninger for overholdelse af GDPR.

Denne årsrapport er den tredje i rækken fra kommunens DPO og dækker perioden 1. januar 2021 – 31. december 2021.

Årsrapporten giver kommunens politiske ledelse en status for kommunens overholdelse af GDPR baseret på kommunens resultater for GDPR-modenhedsmålingen og kommunens egne oplyste tal for performance i forhold til udvalgte GDPR-områder (herefter kommunens GDPR-nøgletal). Desuden giver DPO'en anbefalinger til kommunens arbejde med databeskyttelse i 2022.

På side 3-8 giver DPO'en en status for kommunens overholdelse af GDPR samt anbefalinger og forslag til kontroller.

Bilag 1 indeholder de samlede resultater for GDPR-modenhedsmålingen, som DPO'en foretog i november 2021. Bilag 2 indeholder kommunens GDPR-nøgletal, som er indsamlet og opgjort i slutningen af 2021. Bilag 3 indeholder sagsstatistik for DPO'ens arbejde i perioden 1. januar 2021 – 31. december 2021.

Den bredere kontekst

Det kan være en udfordring for kommunen at navigere i det databeskyttelsesretlige univers samtidig med, at kerneopgaverne skal løses. GDPR kan indimellem stadig give lidt udfordringer. Det er dog tydeligt at høre på de spørgsmål der indgår hos DPO´en, at GDPR vinder større og større indpas hos de enkelte ansatte og der langsomt er ved at blive opbygget en grundlæggende viden på området. Hos kommunernes GDPR-konsulenter ser man ligeledes en udvikling og et engagement, der medvirker til et løft af compliance-niveauet. Fokus skal fortsat være at reglerne er til for at sikre grundlæggende rettigheder om beskyttelse af persondata og retten til privatliv for borgere eller andre personer, som kommunen behandler oplysninger om. Beskyttelse af persondata og privatliv er en forudsætning for tillid til digitalisering i kommunen, og beskyttelsen skal derfor gå hånd i hånd med den øgede digitalisering, som allerede er i gang i kommunen, og de nye muligheder for yderligere digitalisering og brug af data, som følger med kommunernes digitaliseringsprogram for 2021-2025.

Datatilsynet har i 2021 indstillet tre kommuner til bøder for overtrædelse af GDPR. Alle tre kommuner er indstillet til bøde for ikke at leve op til kravene om et passende sikkerhedsniveau efter GDPR: Frederiksberg 100.000 kr. for ej at have etableret passende sikkerhedsforanstaltninger i tandplejesystem, Favrskov 75.000 kr. for manglende kryptering af harddisk og Vejle 200.000 kr. ligeledes for manglende navne- og adressebeskyttelse i tandplejesystem.

I 2021 kom Datatilsynet endvidere med en afgørelse om DPO´ens opgavevaretagelse i Den Storkøbenhavnske Digitaliseringsforening. Datatilsynet fandt, at kommunernes brug af DPO-funktionen lå inden for rammerne af GDPR.

EU-domstolens afgørelse fra juli 2020 (Schrems II), omkring overførsel af personoplysninger til USA og andre usikre tredjelande (dvs. ikke EU-lande), trak fortsat lange tråde ind i 2021. Med de endelige anbefalinger den 21. juni 2021 fra Det Europæiske Databeskyttelsesråd (EDPB), troede de fleste, at nu havde man nøglen til hvordan kravene efterleves, som ifølge EU-domstolen gælder ved overførsel af personoplysninger til USA og øvrige usikre 3. lande uden for EU. Anbefalingerne har dog fortsat efterladt et stort rum for fortolkning. EU-dommen (Schrems II) skaber derfor fortsat udfordringer for kommunen, idet flere af kommunens systemer bygger på aftaler, som er indgået med databehandlere eller underdatabehandlere i USA.

Det første konkrete eksempel fra praksis, har vist sig i Helsingør-sagen fra efteråret 2021, hvor Datatilsynet har ført tilsyn med kommunens brug af Googles Cromebooks til skolernes elever. Det er således værd at bemærke, at Datatilsynet som minimum forventer, at der foretages en risikovurdering, men at der ligeledes foretages en Transfer Impact Assessement (TIA) dvs. en vurdering af beskyttelsesniveauet i det land man overfører til.

Andreas Drægert, DPO for Rødovre Kommune, 30-03-2022

Status for overholdelse af GDPR i kommunen

Ændringer i 2021

Tidligere rapporter har indeholdt en tommel, tal for modenhed og farveangivelse fra skalaen for hvert målepunkt. I årsrapporten for 2021 er det vurderet unødvendigt og er derfor fjernet for de enkelte målepunkter.
I anbefalingerne er angivelserne uændrede.

Resultater for GDPR-modenhedsmåling 2021

DPO'en gennemførte i november 2021 den årlige GDPR-modenhedsmåling, som måler på kommunens niveau og forudsætninger i forhold til at kunne overholde GDPR. Der er målt på 35 modenhedskriterier, som afspejler krav efter GDPR eller på anden måde har betydning for implementering af GDPR og drift af GDPR-opgaver i kommunen (fx ledelsesmæssig opbakning).

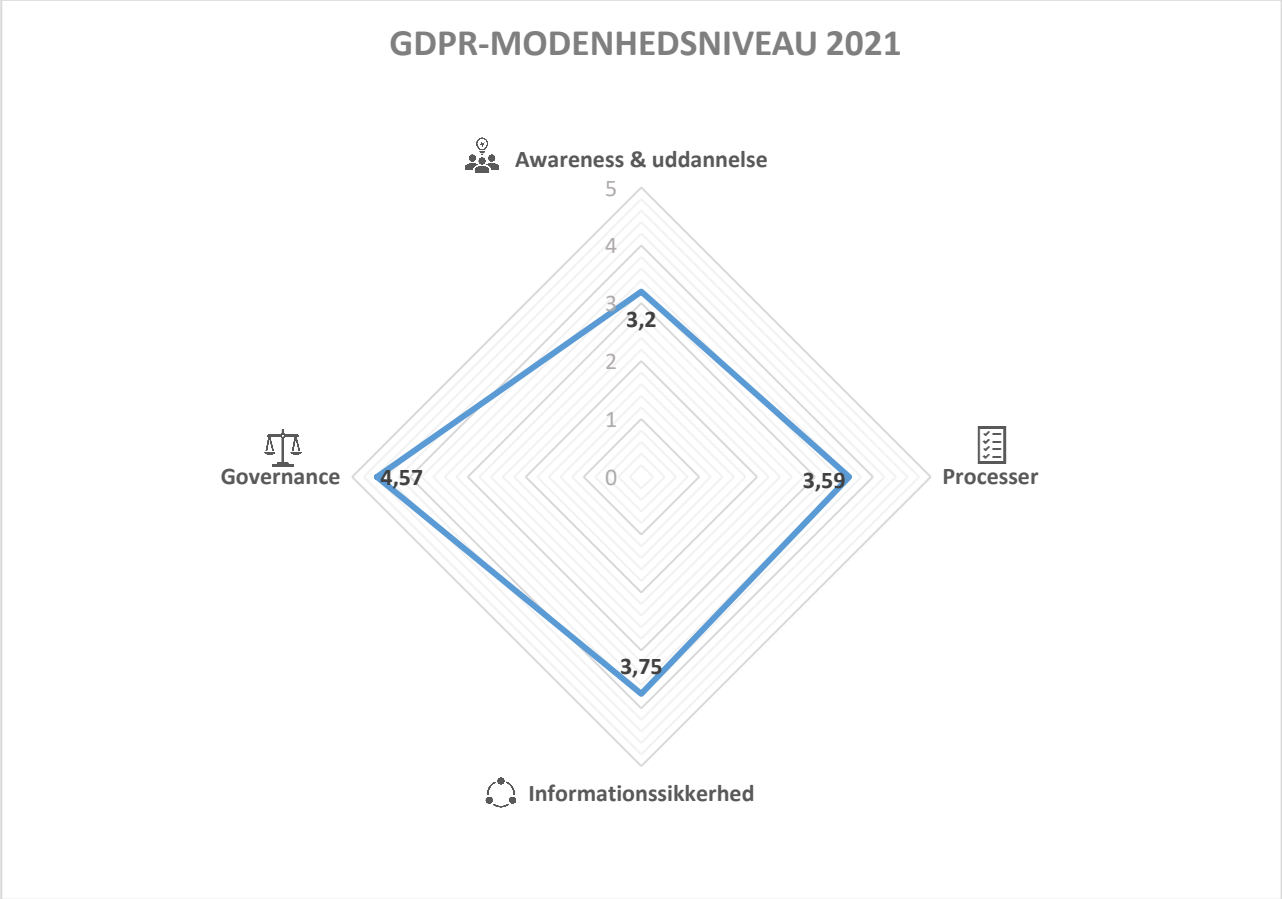
Målingen udgøres af besvarelser fra udpegede respondenter i kommunen (selvevaluering), og resultaterne udgør kommunens GDPR-modenhedsniveau for 2021.

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

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

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

Model 1: Gennemsnitsresultater for 2021 fordelt på fire hovedområder[2]



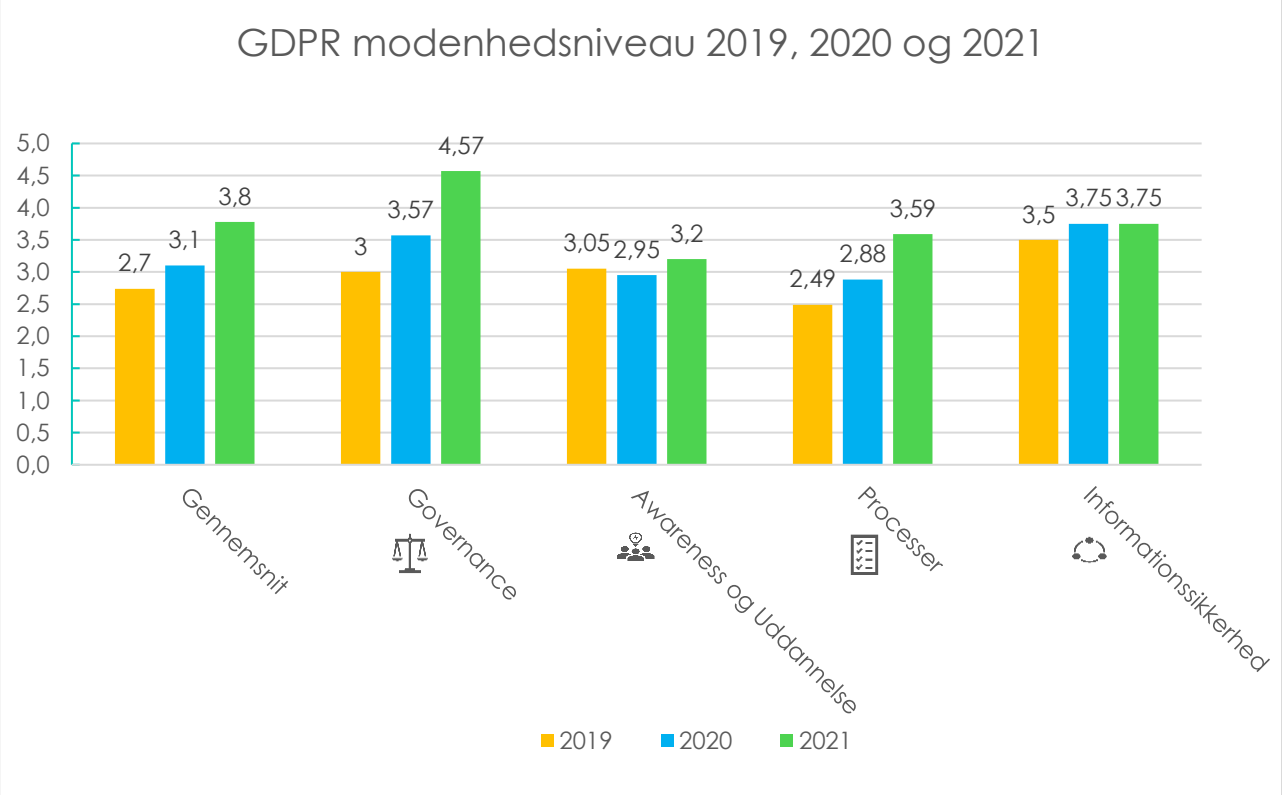
DPO'ens vurdering

Samlet set viser resultatet for GDPR-modenhedsmålingen i 2021, at kommunens GDPR-modenhedsniveau er højere end 3 i forhold til de overordnede 4 kriterier for opfyldelse af GDPR-krav. Ydermere er der særligt på Governance-området sket en markant forbedring siden målingen i 2020. Det indikerer, at kommunen på tidspunktet for målingen overholder mange GDPR-krav og ift. Governance ikke bare overholder minimumskrav, men har fuldt implementeret GDPR og kan begynde at optimere og forbedre arbejdet.

Kommunens gennemsnitlige GDPR-modenhedsniveau i 2021 er 3,8, og modenheden er dermed øget med 0,7 sammenlignet med målingen i 2020, hvor gennemsnitsniveauet var 3,1. Det øgede modenhedsniveau afspejler, at kommunen har arbejdet målrettet med flere af DPO'ens anbefalinger fra sidste år, og at kommunen har rykket sig væsentligt. Kommunens indsats har således udmøntet sig i målbare resultater, og betyder fremadrettet at kommunen kan begynde at fokusere på at finde et niveau for drift, der også kan indeholde optimering og forbedring.

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

Model 2: Resultat af GDPR-modenhedsmåling i 2021 sammenlignet med målingen i 2020 og 2019[3]



Kommunens GDPR-nøgletal 2021

Henvendelser fra borgere

Kommunen har modtaget 13 henvendelser fra borgere, som har gjort brug af deres rettigheder efter GDPR til at få indsigt i egne persondata. Det er en stigning sammenlignet med 2020, hvor kommunen modtog 6 henvendelser. Kommunen har håndteret alle henvendelserne inden for 30-dagesfristen efter tidspunktet for modtagelsen af anmodningen.

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

Brud på persondatasikkerheden

Kommunen har registreret 36 brud på persondatasikkerheden i 2021. Det er en markant stigning sammenlignet med 2020, hvor kommunen registrerede 16 brud på persondatasikkerheden. I 23 ud af de 36 brud i 2021 har kommunen foretaget anmeldelse til Datatilsynet, heraf er samtlige brud anmeldt til Datatilsynet inden for den rette frist, dvs. inden 72 timer efter kommunen har fået kendskab til bruddet. (Kommunen har i 21 ud af de i alt 36 brud foretaget underretning af de borgere, der har været udsat for brud på sikkerheden ved kommunens behandling af deres persondata.

Registrering af brud på sikkerheden er en dynamisk størrelse og afspejler ikke kun kommunens evne til at varetage sikkerhed. Brud opstår også hos leverandører, hvilket kommunen meget sjældent kan forhindre. Det er generelt DPO'ens vurdering, at kommunen har håndteret brud på persondatasikkerheden i overensstemmelse med GDPR.

[3] Der henvises til bilag 1 for de samlede resultater for GDPR-modenhedsmålingerne i 2021, 2020 og 2019.

Nye it-løsninger og inddragelse af DPO'en
Kommunen har anskaffet 22 nye it-løsninger til brug for behandling af persondata, hvoraf DPO'en har været inddraget i 7 tilfælde. Der er til sammenligning med 2020 både anskaffet flere løsninger, og DPO'en er inddraget i færre tilfælde.

Det er DPO'ens vurdering, at kommunens procedure for inddragelse af DPO'en, i forhold til anskaffelse af nye it-løsninger, altid skal reflektere kompleksiteten af behandlingen af personoplysninger i et system. Jo højere kompleksitet, desto større incitament til inddragelse.

Dette gælder også, før kommunen offentliggør udbudsmateriale, hvor kommunen skal stille krav til løsningerne og skal tage højde for privacy by design. Systemer til brug for behandling af persondata skal fra start være designet således, at krav efter GDPR kan overholdes, og persondata kan beskyttes, og der er en betydelig ressourcebesparelse ved at indtænke GDPR så tidligt som muligt sammenlignet med det ressourcetræk, der kan være forbundet med efterfølgende at skulle rette op og tilpasse løsninger mv. Hertil kommer den retssikkerhedsmæssige værdi for borgere, hvis oplysninger kommunen skal behandle i disse systemer.

Risikostyring
Kommunen har gennemført 333 risikovurderinger i forhold til behandling af persondata. Kommunen har gennemført 0 konsekvensanalyser vedrørende databeskyttelse i forhold til persondatabehandling samt gennemført 1 tærskelvurdering (dvs. en vurdering af, om kommunen er underlagt krav om gennemførelse af en konsekvensanalyse vedrørende databeskyttelse forud for behandling).

Det er DPO'ens vurdering, at der er lagt et meget stort arbejde i at få risikovurderet den mængde af behandlingsaktiviteter.
Rødovre Kommune har mange it-systemer og mange forskellige måder at behandle personoplysninger på. En så stor diversitet nødvendiggør et overblik over kommunens risici. Risikostyring er derfor en central komponent i en risikobaseret tilgang til GDPR, som forudsætter løbende risikovurderinger i forhold til persondatabehandling og implementering af passende sikkerhedsforanstaltninger, hvis risiciene for de registrerede er for høj. Uden risikovurderinger, er det ikke muligt at vurdere, om der er en passende beskyttelse af persondata. Beskyttelse af persondata og privatlivet er en forudsætning for tillid til digitalisering i kommunen, og beskyttelsen skal derfor gå hånd i hånd med den øgede digitalisering, som allerede er i gang i kommunen, og de nye muligheder for yderligere digitalisering og brug af data. Kommunen har med dette arbejde taget et godt skridt mod at få lavet en kritisk forudsætning for arbejdet med GDPR. Det anbefales at Rødovre Kommune aktivt ajourfører deres risikooverblik og aktivt benytter sig af deres risikovurderinger i arbejdet med at prioritere og håndtere risici.

Tilsyn fra Datatilsynet og intern kontrol med overholdelse af GDPR
Datatilsynet har ikke iværksat tilsyn med kommunen i 2021. I et tilfælde har Datatilsynet fulgt op over for kommunen. Kommunen har i løbet af 2021 iværksat interne kontroller og et såkaldt årshjul, der dokumenterer efterlevelse af krav i GDPR.

Det er positivt, at kommunen har iværksat interne kontroller og et årshjul, da det er en forudsætning for at sikre kommunens GDPR-compliance, når der henses til det store omfang af persondata og karakteren af persondata, som håndteres i kommunen. Det er et krav, at kommunen løbende skal tjekke overholdelsen af GDPR med interne kontroller. DPO'en fastholder sin anbefaling om at kommunen bør udvikle et koncept og en årlig plan for stikprøvekontrol efter en risikobaseret tilgang og foretage flere stikprøvekontroller med overholdelse af politikker for beskyttelse af persondata og GDPR i kommunen.

Kommunens GDPR-ressourcer
Kommunen har i alt 3 dedikerede årsværk og 6 ikke dedikerede årsværk til arbejdet med GDPR. Dette er en opnormering på 1 årsværk sammenlignet med 2020.

Det er DPO'ens opfattelse, at ressourcerne udgør et godt udgangspunkt for arbejdet med implementering af GDPR og drift af GDPR-opgaver i kommunen.

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

DPO'ens anbefaling samt forslag til kontrol

DPO'ens anbefaling på baggrund af kommunens GDPR-nøgletal 2021 og GDPR-modenhedsmåling 2021	Forslag til kontrol
• Sikkerhedstest: 	Få etableret en nedskrevet procedure, som sikrer, at kommunen løbende afprøver og vurderer implementerede foranstaltningers effektivitet.
• Privacy by design, privacy by default: 	Få etableret en nedskrevet procedure, som sikrer, at kommunen har kravspecifikation til systemer, så systemer er indrettet med privatlivsbeskyttelse i deres design og altid slået til som standard.
• Awareness 	Proceduren for awareness gennemgås og der laves en plan for at have en konsistent udrulning af awareness materiale.
• Risikostyring 	Proceduren for risikovurderinger gennemgås og der laves en plan for først at præsentere og derefter for at nedbringe risici i en prioriteret rækkefølge, hvor prioriteringen er at starte med højeste risiko for de registrerede.
• Implementering af passende sikkerhedsforanstaltninger 	Passende sikkerhedsforanstaltninger er de tiltag der nedbringer risici ved risikostyring.
• Sikkerhedsprogram (ISO 27001) 	Sikkerhedsprogrammet bør indeholde kontroller, der sikrer at der rettidigt, jævnligt og ved ændringer følges op på nye og/eller eksisterende risici.
• Konsekvensanalyse vedr. databeskyttelse og tærskelsvurdering 	Proceduren for udarbejdelse af tærskelsvurdering og konsekvensanalyser bør indeholde en beskrivelse af hvordan Rødovre Kommune starter et forløb, inddrager DPO'en og efterfølgende journaliserer det på en måde, så det kan dokumenteres.

Bilag 1

GDPR-modenhedsmåling 2021

Formål

GDPR-modenhedsmålingen af kommunen i november 2021 blev udført som en del af DPO'ens lovpligtige opgave med at overvåge kommunens overholdelse af GDPR.

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

På side 12-24 vises de samlede resultater for GDPR-modenhedsmålingen i 2021 med grønne søjler. For sammenligningens skyld gengives resultaterne for 2020 og 2019 med blå og orange søjler.

Metode

Målingen af GDPR-modenheden er baseret på principper fra den anerkendte AICPA Privacy Maturity Model[4]. DPO'en har modificeret modellens kriterier til kommunal kontekst med primært fokus på GDPR. Data, som ligger til grund for resultaterne i målingen, er baseret på en survey med svar fra respondenter, som kommunen internt har udpeget (selvevaluering).

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

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

Omfang

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

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

Modenhedskriterier

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

Governance

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

Awareness og uddannelse

8. Awareness*
9. Uddannelse*

Processer

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

Informationssikkerhed

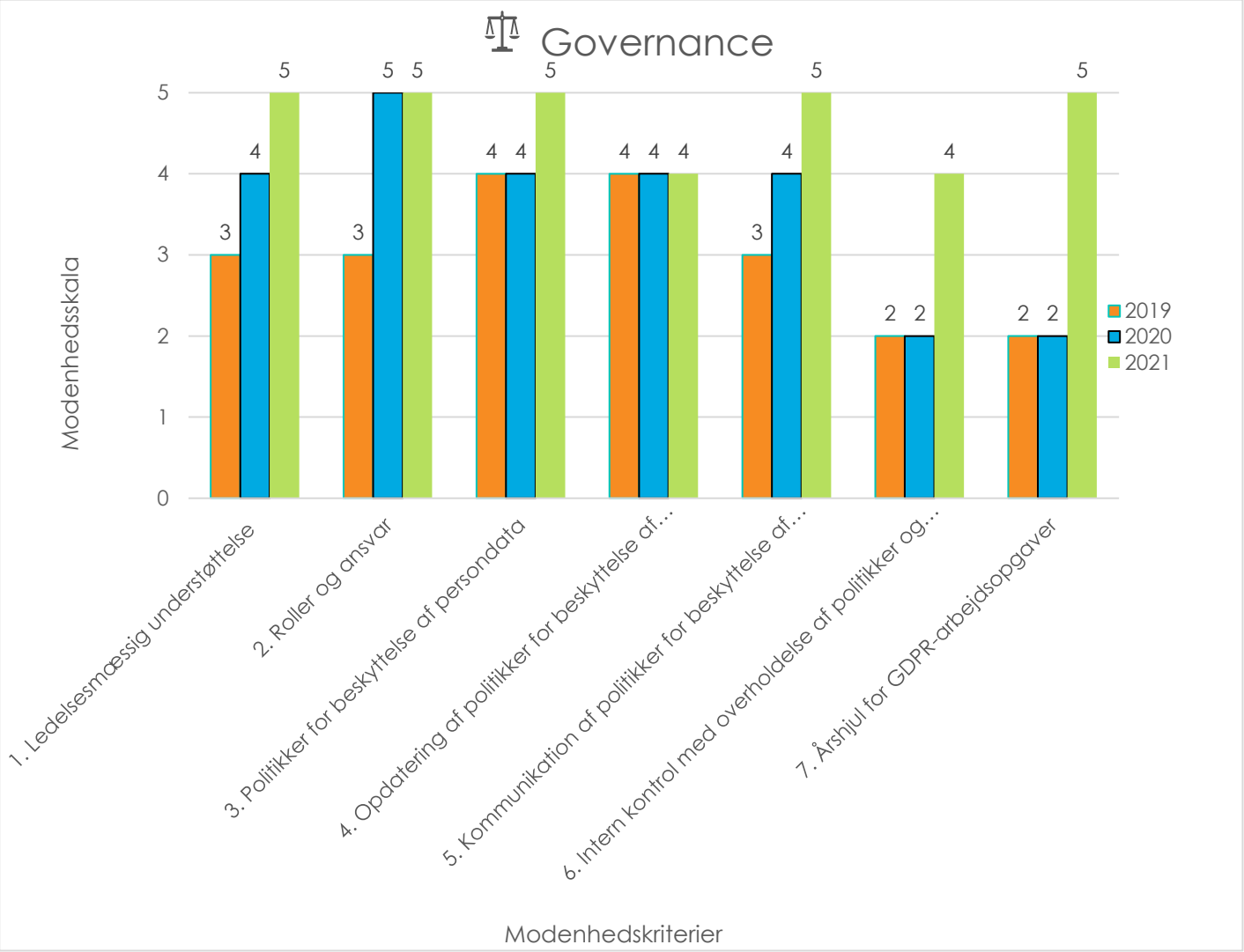
32. Sikkerhedsprogram (ISO27001)
33. Risikovurderinger af kritiske forretningsprocesser (ISO27001)
34. Beredskabsplan
35. Test af beredskabsplan

Målestok

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

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

Governance



Introduktion til governance

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

1. Ledelsesmæssig understøttelse

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

2. Roller og ansvar

Kriteriet afspejler det forhold, at roller og ansvar skal være defineret i kommunen i forhold til implementering og driftsopgaver.

Der er målt på, om roller og ansvar for GDPR-compliance er tydeligt defineret.

3. Politikker for beskyttelse af persondata

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

4. Opdatering af politikker for beskyttelse af persondata

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

5. Kommunikation af politikker for beskyttelse af persondata

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

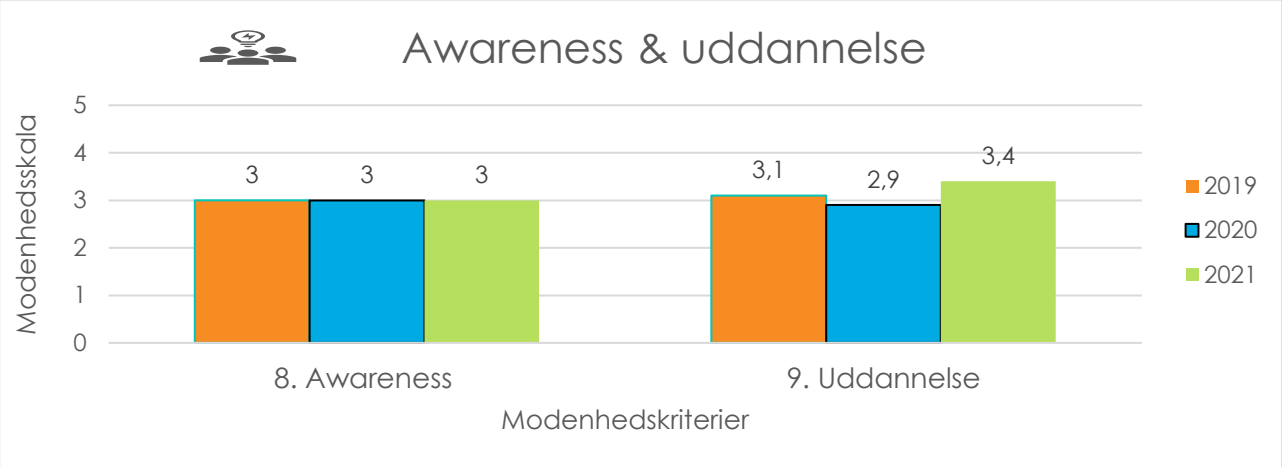
6. Intern kontrol med overholdelse af politikker og GDPR-compliance

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

7. Årshjul for GDPR-arbejdsopgaver

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

Awareness & uddannelse



Introduktion til awareness og uddannelse

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

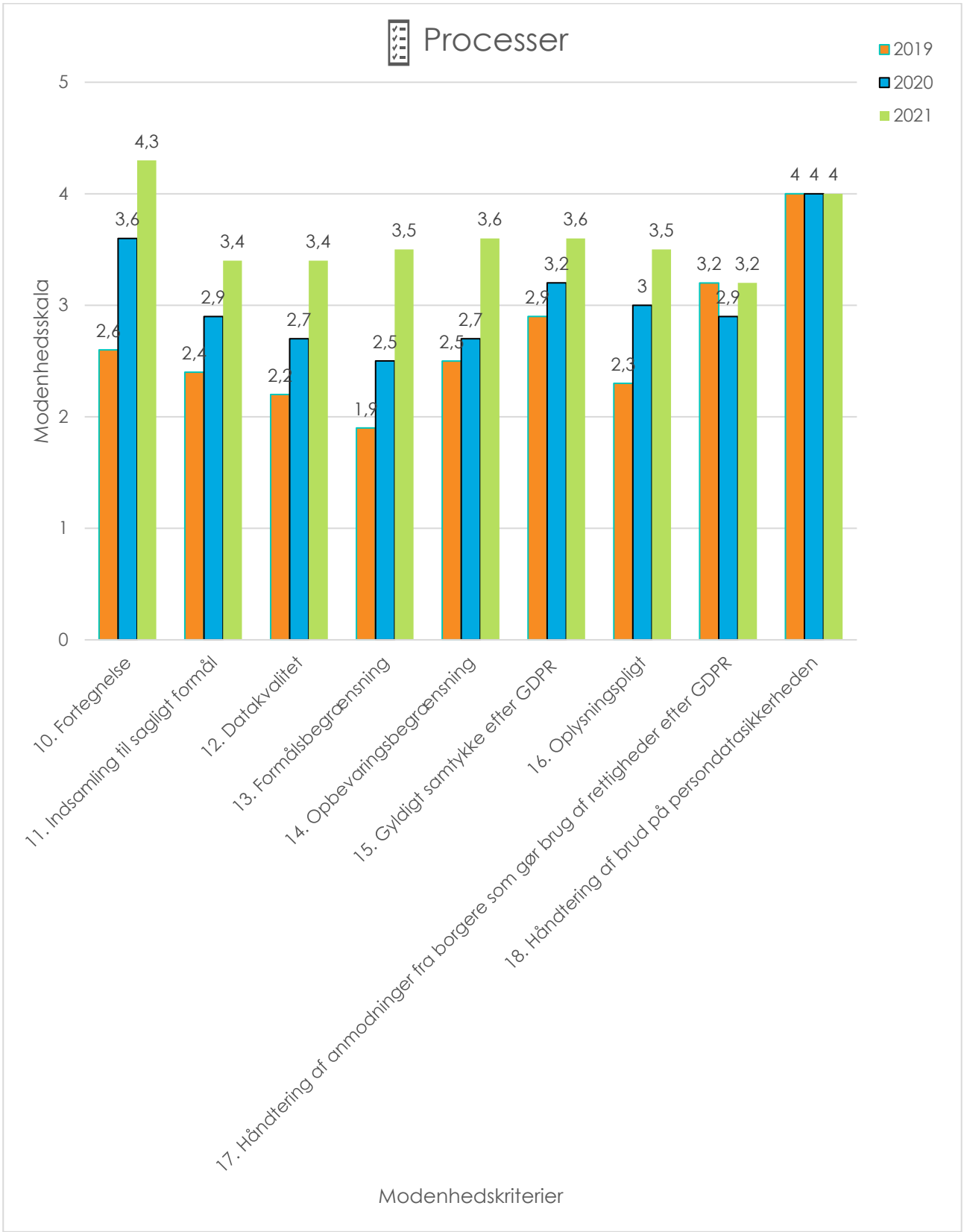
8. Awareness

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

9. Uddannelse

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

Processer


Processer
2019
2020
2021
Modenhedsskala
0
1
2
3
4
5
2,6
3,6
4,3
2,4
2,9
3,4
2,2
2,7
3,4
1,9
2,5
3,5
2,5
2,7
3,6
2,9
3,2
3,6
2,3
3
3,5
3,2
2,9
3,2
4 4 4
10. Fortegnelse
11. Indsamling til sagligt formål
12. Datakvalitet
13. Formålsbegrænsning
14. Opbevaringsbegrænsning
15. Gyldigt samtykke efter GDPR
16. Oplysningspligt
17. Håndtering af anmodninger fra borgere som gør brug af rettigheder efter GDPR
18. Håndtering af brud på persondatasikkerheden
Modenhedskriterier

Introduktion til processer

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

10. Fortegnelse

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

Behandlingsprincipperne efter GDPR

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

11. Indsamling til sagligt formål (dataminimering)

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

12. Datakvalitet

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

13. Formålsbegrænsning

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

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

14. Opbevaringsbegrænsning

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

15. Gyldigt samtykke efter GDPR

Kriteriet afspejler det forhold, at behandling af persondata, som er sker på baggrund af samtykke fra borgere til, at kommunen må

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

16. Oplysningspligt

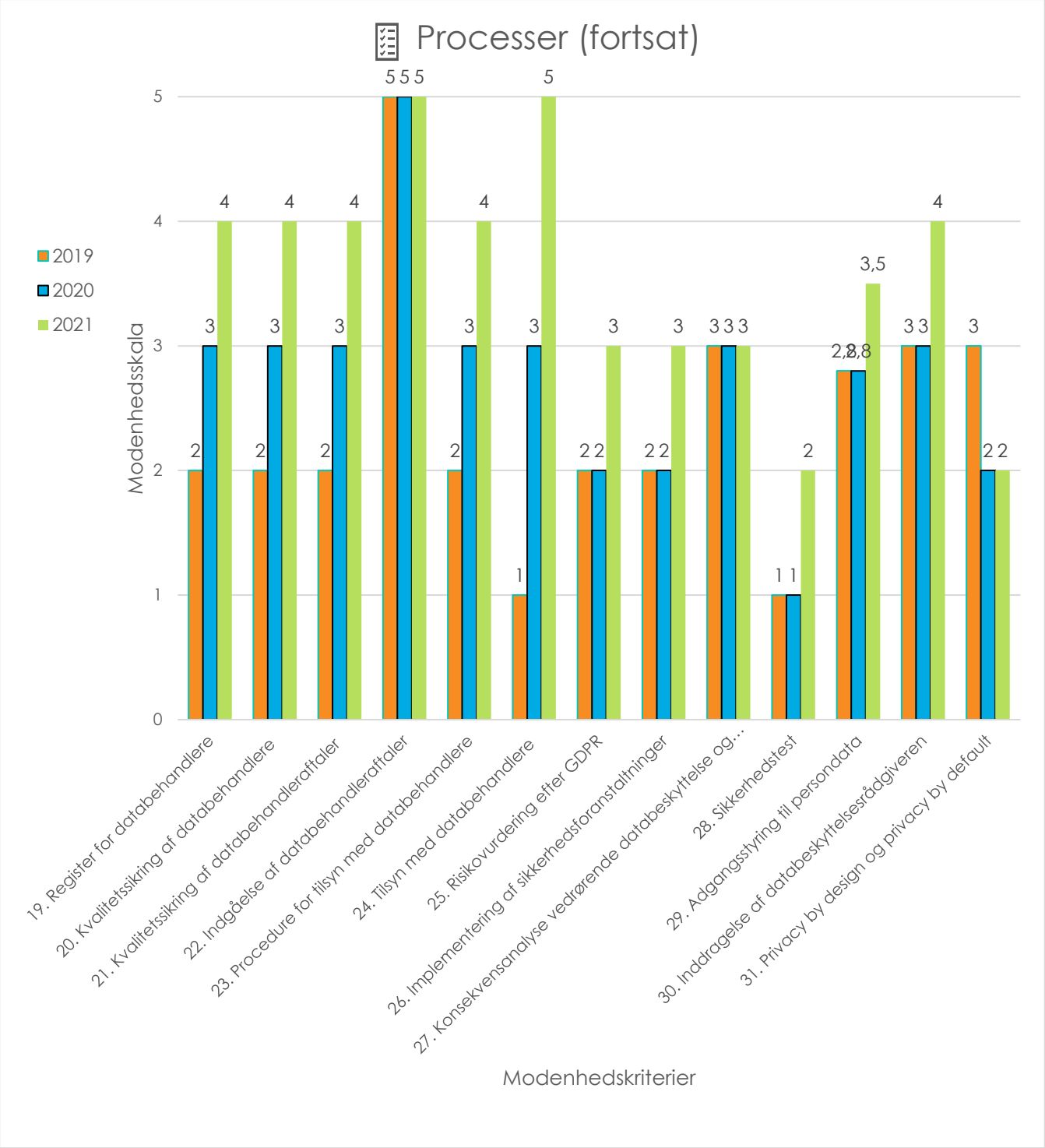
Kriteriet afspejler det forhold, at borgere (og andre personer), som kommunen behandler persondata om, skal orienteres skriftligt om behandlingsformål og behandlingshjemmel og øvrige forhold i forbindelse med kommunens første indsamling af persondata om vedkommende. Der er målt på, om der i kommunens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

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

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

18. Håndtering af brud på persondatasikkerheden

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



19. Register for databehandlere

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

20. Kvalitetssikring af databehandlere (due diligence)

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

målt på, om der i kommunen er etableret en nedskrevet procedure, som sikrer, at kommunen kan kvalitetssikre databehandlere, inden der indgås en databehandleraftaler.

21. Kvalitetssikring af databehandleraftaler

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

22. Indgåelse af databehandleraftaler

Kriteriet afspejler det forhold, at kommunen skal indgå databehandleraftaler med alle databehandlere, som behandler persondata på vegne af kommunen. Der er målt på, om kommunen har indgået databehandleraftaler med sine databehandlere (målt procentvist)[5].

23. Procedure for tilsyn med databehandlere

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

24. Tilsyn med databehandlere

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

25. Risikovurderinger efter GDPR

Kriteriet afspejler det forhold, at kommunen skal gennemføre risikovurderinger med fokus på persondatabeskyttelse for de borgere (og andre personer), som kommunen behandler oplysninger om. Det følger af ansvarlighedsprincippet, at kommunen skal kunne påvise, at der er gennemført risikovurderinger, som lever op til kravene efter GDPR. Der er målt på, om kommunen gennemfører dokumenterede risikovurderinger i overensstemmelse med GDPR.

26. Implementering af sikkerhedsforanstaltninger

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

27. Konsekvensanalyse vedrørende databeskyttelse og tærskelvurdering

Kriteriet afspejler det forhold, at kommunen skal gennemføre en konsekvensanalyse vedrørende databeskyttelse forud for behandling af persondata, hvis det er sandsynligt, at behandlingen vil indebære en høj risiko for brud på rettigheder og frihedsrettigheder for borgere (og andre personer), der skal behandles persondata om. En konsekvensanalyse vedrørende databeskyttelse skal nedbringe uacceptabel høj risiko for rettigheder og frihedsrettigheder for de borgere (og andre personer), der skal behandles persondata om, forud for behandling. Det er nødvendigt at foretage en tærskelvurdering af en planlagt persondatabehandlings karakter, formål, sammenhæng og omfang for at identificere, om

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

det er sandsynligt, at den pågældende planlagte behandling vil indebære en høj risiko for brud på rettigheder og frihedsrettigheder for borgere (og andre personer), der skal behandles persondata om. Der er målt på, om der foreligger en nedskrevet procedure for tærskelvurdering, som sikrer, at kommunen kan identificere, om planlagte nye behandlinger af persondata i kommunen er underlagt krav om gennemførelse af en konsekvensanalyse.

28. Sikkerhedstest

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

29. Adgangsstyring til persondata

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

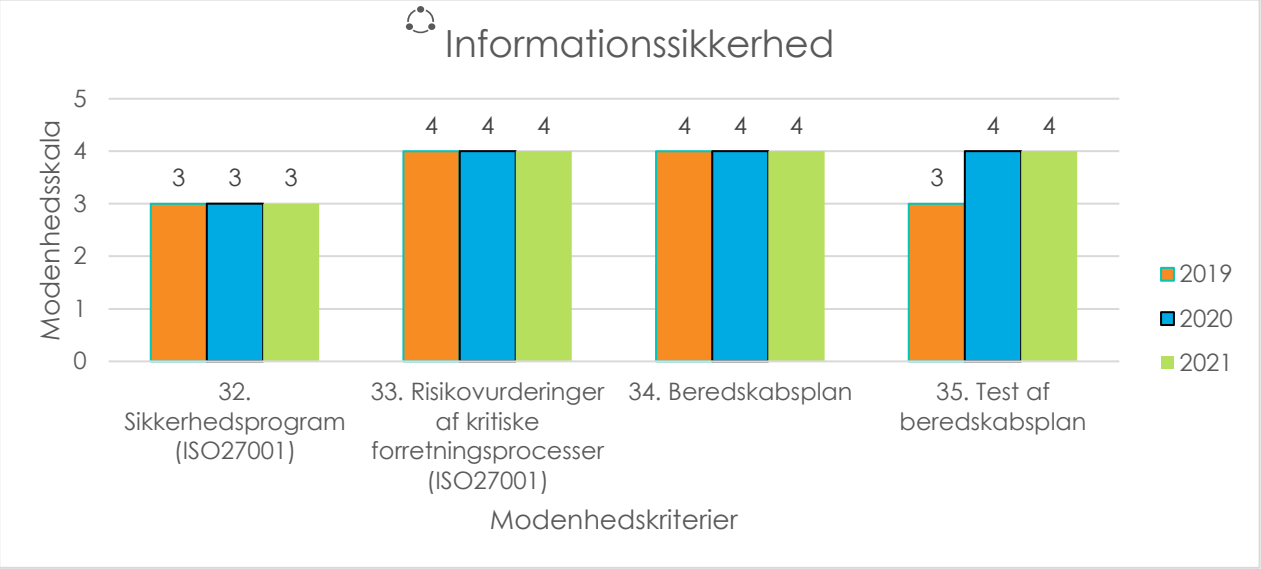
30. Inddragelse af DPO'en

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

31. Privacy by design og privacy by default

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

Informationssikkerhed



Introduktion til informationssikkerhed

Det følger af den fællesoffentlige digitaliseringsstrategi for 2016-2021, at kommunerne skal følge principperne i ISO27001. ISO27001 er en international standard for informationssikkerhed, som har til formål at bevare fortrolighed, integritet og tilgængelighed af informationsaktiver i en organisation. GDPR-modenhedsmålingen omfatter enkelte kriterier om informationssikkerhed, som udover at bevare informationsaktiver også har betydning for beskyttelse af persondata. Kriterierne afspejler ikke direkte krav efter GDPR.

32. Sikkerhedsprogram (ISO27001)

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

33. Risikovurderinger af kritiske forretningsprocesser

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

34. Beredskabsplan

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

35. Test af beredskabsplan

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

Bilag 2

Kommunens GDPR-nøgletal for 2021

DPO'en har indsamlet kommunens GDPR-nøgletal for 2021 (kommunens egne oplyste tal for performance i forhold til udvalgte GDPR-områder). I tabellerne medtages kommunens nøgletal for 2020

Henvendelser fra borgere, som gør brug af rettigheder efter GDPR

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

Kommunen har modtaget 13 anmodninger om indsigt i egne persondata i 2021. Det er en markant stigning sammenlignet med 2020, hvor kommunen modtog 6 anmodninger. Kommunen har ikke ført statistik over henvendelse fra borgere, som har gjort brug af andre rettigheder efter GDPR end indsigt i egne persondata.[6]

Kommunens nøgletal viser, at kommunen har behandlet alle henvendelser fra borgere, som har anmodet om indsigt i egne persondata, inden for 30-dages fristen efter tidspunktet for modtagelsen af anmodningen.

Brud på persondatasikkerheden

Antal	2020	**2021**
Registrerede brud på persondatasikkerheden	19	36
Brud anmeldt til Datatilsynet	12	23
Brud hvoraf der er sket underretning til borgere (eller andre personer), som er genstand for bruddet	12	21[7]
Anmeldelser til Datatilsynet inden for lovfristen på 72 timer	11	23

Kommunen har registreret 36 brud på persondatasikkerheden i 2021. Det er en markant stigning sammenlignet med 2020, hvor kommunen registrerede 19 brud på persondatasikkerheden. Hvorfor det er tilfældet, kan skyldes mange ting. Kommunen har anmeldt 12 af i alt 19 brud til Datatilsynet samt underrettet borgere (eller andre personer), som er genstand for bruddet i alle tilfælde hvor bruddet er anmeldt til Datatilsynet (12 ud af 12 brud). Dette indikerer, at kommunen er blevet skarpere i vurderingen af, hvornår brud skal anmeldes til Datatilsynet og underrettes om til borgere (eller andre personer), som er genstand for bruddet.

Kommunens nøgletal for 2021 viser endelig, at kommunen er blevet markant bedre til at anmelde brud til Datatilsynet inden for lovfristen (11 ud af i alt 12 brud) sammenlignet med 2019/18, hvor kommunen anmeldte 13 ud af 45 brud inden for lovfristen.

[6] Det er ikke et krav efter GDPR at føre statistik med henvendelser fra borgere, som gør brug af deres rettigheder efter GDPR, men statistik kan anvendes i forbindelse med intern kontrol med, om henvendelser håndteres korrekt i kommunen.

[7] Der er 21 sikkerhedsbrud, hvor der i alt er underrettet 60 registrerede.

Nye it-løsninger og inddragelse af DPO'en

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

Kommunen har i 2021 anskaffet i alt 22 nye it-løsninger til brug for behandling af persondata, og DPO'en er blevet inddraget i 7 tilfælde. Det er en stigning i antal, i forhold til inddragelsen af DPO'en ved anskaffelse af nye it-løsninger i 2020. Ift. inddragelse af DPO'en ved anskaffelse af nye it-løsninger i 2021, er der sket en stigning i antal og også forholdsvis fra 2020.

Risikostyring – antal risikovurderinger, tærskelvurderinger og konsekvensanalyser

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

Kommunen har gennemført 333 risikovurderinger i forhold til behandling af persondata. Kommunen har gennemført 0 konsekvensanalyser vedrørende databeskyttelse i forhold til persondatabehandling, samt gennemført 1 tærskelvurdering (dvs. en vurdering af, om kommunen er underlagt krav om gennemførelse af en konsekvensanalyse vedrørende databeskyttelse, forud for behandling).

Det er DPO'ens vurdering, at der er lagt et meget stort arbejde i at få risikovurderet den mængde af behandlingsaktiviteter. Rødovre Kommune har et meget stort omfang af persondata og karakteren af persondata inkluderer mange både følsomme og fortrolige data. Derudover har Rødovre Kommune mange it-systemer, og mange forskellige måder at behandle personoplysninger på(fagområder).
En så stor diversitet, nødvendiggør et overblik over kommunens risici. Risikostyring er derfor en central komponent i en risikobaseret tilgang til GDPR, som forudsætter løbende risikovurderinger i forhold til persondatabehandling og implementering af passende sikkerhedsforanstaltninger, hvis risiciene for persondata er for høj.
Uden risikovurderinger, er det ikke muligt at vurdere, om der er en passende beskyttelse af persondata. Beskyttelse af persondata og privatlivet, er en forudsætning for tillid til digitalisering i kommunen, og beskyttelsen skal derfor gå hånd i hånd med den øgede digitalisering, som allerede er i gang i kommunen. Dette skal ses sammen med muligheder for yderligere digitalisering og brug af data. Kommunen har med dette arbejde, sikret en kritisk forudsætning for arbejdet med GDPR. Det anbefales, at Rødovre Kommune aktivt ajourfører deres risikooverblik og aktivt benytter sig af deres risikovurderinger i arbejdet med at prioritere og håndtere risici. God risikostyring forudsætter herudover, løbende gennemførelse af tærskelvurderinger i forhold til planlagte nye behandlinger af persondata i kommunen, samt hvis påkrævet, gennemførelse af konsekvensanalyser vedrørende databeskyttelse.

Tilsyn/henvendelser/påtaler og bøder fra Datatilsynet

Antal	2020	2021
Tilsyn	0	0
Emner for tilsyn:		
Øvrige skriftlige henvendelser/forespørgsler fra Datatilsynet/anmodning fra Datatilsynet om uddybning af spørgsmål vedrørende brud på persondatasikkerheden	-	1
Påtaler/påbud/kritik fra Datatilsynet	Tilsyn 2: Datatilsynet udtalte	0

	alvorlig kritik af kommunen.	
Bøder fra Datatilsynet	0	0

Datatilsynet har ikke iværksat tilsyn af kommune i 2021.

Datatilsynet har i et tilfælde fulgt op over for kommunen og bedt om en uddybning.

Interne kontroller i kommunen med overholdelse af GDPR

Antal	2020	**2021**
Planlagte tilsyn	0	0
Emne for planlagt tilsyn		
Gennemførte tilsyn		
Emne for gennemført tilsyn		

Kommunen har i 2021 ikke gennemført planlagte kontroller med overholdelse af GDPR i kommunen, men det er positivt, at kommunen har iværksat interne kontroller og et årshjul, da det er en forudsætning for at sikre kommunens GDPR-compliance, når der henses til det store omfang af persondata og karakteren af persondata, som håndteres i kommunen. Det er et krav, at kommunen løbende skal tjekke overholdelsen af GDPR med interne kontroller. DPO'en fastholder sin anbefaling om at kommunen bør udvikle et koncept og en årlig plan for stikprøvekontrol efter en risikobaseret tilgang og foretage flere stikprøvekontroller med overholdelse af politikker for beskyttelse af persondata og GDPR i kommunen.

Kommunens GDPR-ressourcer

Antal	2020	**2021**
Dedikerede årsværk til implementering og drift af GDPR	2	3[8]
Øvrige årsværk til implementering og drift af GDPR	6	6

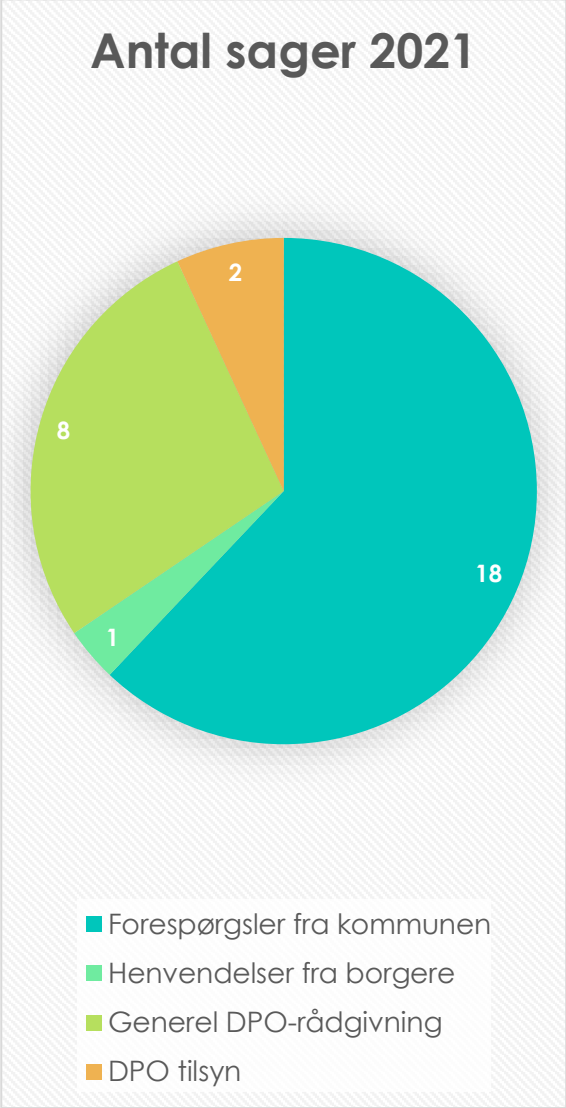
Kommunen har i alt 3 dedikerede årsværk og 6 ikke dedikerede årsværk til arbejdet med GDPR. Dette er en opnormering på 1 årsværk sammenlignet med 2020.

Det er DPO'ens opfattelse, at ressourcerne udgør et godt udgangspunkt for arbejdet med implementering af GDPR og drift af GDPR-opgaver i kommunen.

[8] De tre dedikerede årsværk består af 2 fuldtidsstillinger i GDPR teamet, og det 3. årsværk er sammensat af ressourcer fra bl.a. it-drift, juridisk enhed og digital udvikling.

Bilag 3

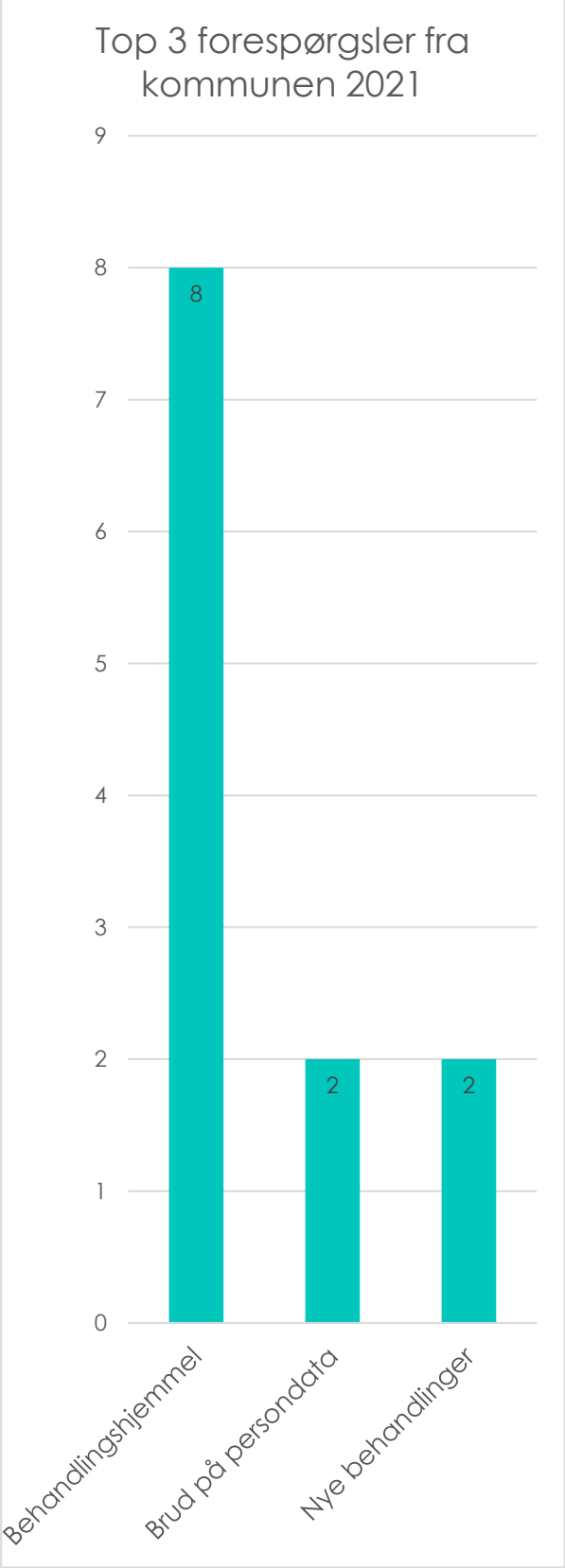
Sagsstatistik for DPO'ens arbejde



Antal sager

DPO'en har i perioden 1. januar 2021 til og med 31. december 2021 oprettet i alt 28 sager, som er fordelt på sagskategorierne: forespørgsler fra kommunen (18 sager), henvendelser fra borgere (1 sag), generel DPO-rådgivning (8 sager) samt DPO-tilsyn, som omfatter DPO'ens tilsyn med kommunen, og tilsyn med kommunens overholdelse af kravene til tv-overvågning (i alt 2 tilsyn).

Hyppigste forespørgsler fra kommunen

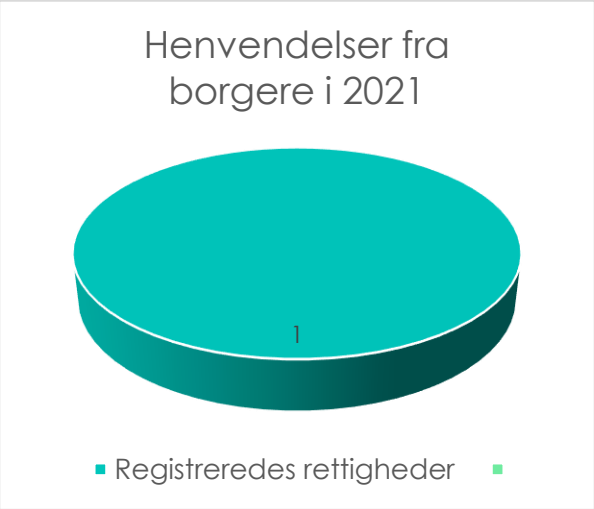


Den hyppigste forespørgsel handler om behandlingshjemmel, hvor DPO'en har modtaget 8 forespørgsler fra kommunen.

Næsthyppigste forespørgsel handler om brud på persondata, hvor DPO'en har modtaget 2 henvendelser.

Herefter kommer forespørgsler, der handler om nye behandlinger hvor DPO'en har modtaget 2 forespørgsler.

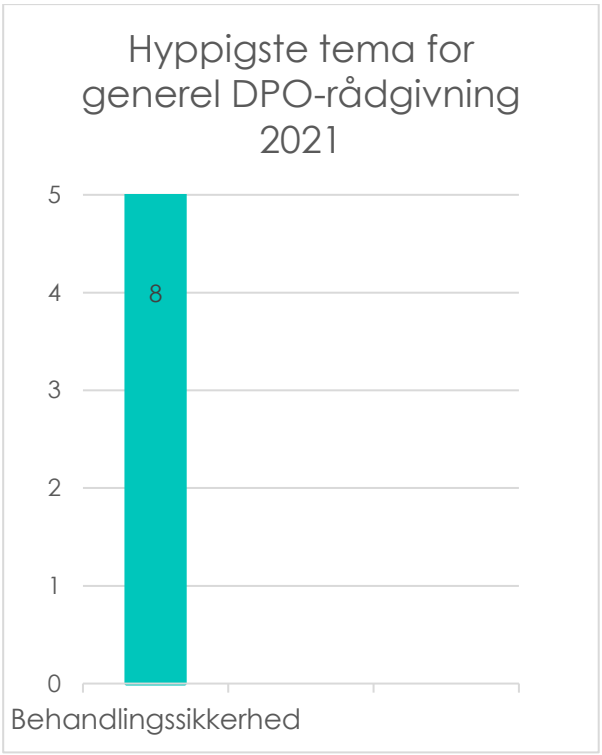
Henvendelser fra borgere



DPO'en har modtaget 1 henvendelse. Henvendelsen har været om den oplysningsseddel kommunen udsender til borgerne, der forklarer behandling af personoplysninger og rettigheder.

Generel DPO-rådgivning

Sagskategorien generel DPO-rådgivning omfatter sager, hvor DPO'en rådgiver, giver anbefalinger eller holder oplæg for kommunerne i Den Storkøbenhavnske Digitaliseringsforening, som er omfattet af DPO-funktionen[9].



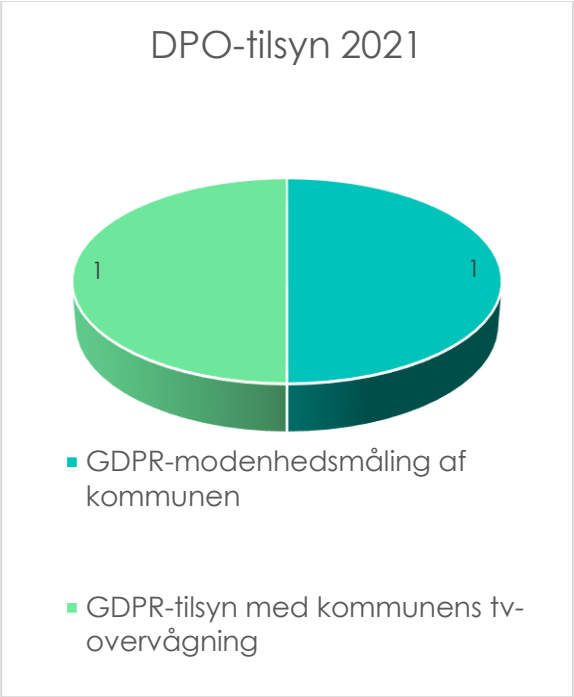
Det hyppigste tema for generel DPO-rådgivning vedrører behandlingssikkerhed. r fx har DPO'en udsendt en opdatering til trusselskataloget for kommunerne i Den Storkøbenhavnske Digitaliseringsforening til brug i risikovurderinger.

DPO'en har rådgivet kommunerne om Schrems II – dommen., Emnet har også affødt både fortolkninger fra KL samt den seneste vejledning i tredjelands-overførsler fra EDPB (Det Europæiske Databeskyttelsesråd), som er blevet behandlet på fortolkningsmøder i foreningen.

DPO'en har faciliteret en præsentation af en kommunes konkrete brug af Google Workspace og rådgivet kommunerne i kravene til brugen af Google Workspace.

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

DPO-tilsyn



DPO'en har ført tilsyn med kommunens overholdelse af GDPR ved gennemførelse af GDPR-modenhedsmålingen i november 2021 (se bilag 1).

DPO'en har desuden i 3. kvartal 2021 gennemført et enkelt tilsyn med overholdelse af GDPR-kravene i forbindelse med kommunens brug af tv-overvågning.

Møder i 2021

DPO'ens fysiske mødeaktivitet har været begrænset i 2021 grundet COVID-19-restriktioner. DPO'en har i stedet deltaget i ad hoc-møder på Teams, blandt andet om modenhedsmålinger etc. samt deltaget regelmæssigt i onlinemøder (såkaldte GDPR-fortolkningsmøder) for sikkerhedskoordinatorerne fra kommunerne i Den Storkøbenhavnske Digitaliseringsforening.

Leverancer

DPO'en har i 2021 brugt en del arbejde på at følge og dokumentere, samt facilitere viden om brugen af Google Workspace til skolerne i DSD. DPO'en har udsendt en tjekliste til at foretage en såkaldt TIA(transfer impact assessment), så kommunen kan varetage dette. DPO'en har opdateret og udsendt et trusselskatalog til brug for risikovurderinger. Der er i den forbindelse også blevet faciliteret en arbejdsgruppe, der er mundet ud i et fælles projekt om risikovurderinger, som alle kommuner kan gøre brug af.

Leverancer 2021

- ✓ Afholdt præsentation om brugen af Google Workspace
- ✓ Faciliteret arbejdsgruppe om fælles risikovurderinger i kommunerne
- ✓ Udsendt tjekliste til at lave transfer impact assessment ved 3. lands-overførsler
- ✓ Opdateret trusselskatalog til risikovurderinger
- ✓ Påbegyndt udsendelse af det månedlige DSD Nyhedsbrev