



DATABESKYTTELSESRÅDGIVERENS ÅRSRAPPORT 2023



Afsender:

DPO-funktionen i Den Storkøbenhavnske Digitaliseringsforening

Modtager:

Kommunalbestyrelsen i Rødovre Kommune

Indhold

Indledning	2
Databeskyttelsesrådgiverens bemærkninger og anbefalinger.....	3
Opsummering.....	3
Bilag 1: Status for overholdelse af GDPR i kommunen.....	4
Bilag 2: Data fra modenhedsmålingen.....	5
Bilag 3: Nøgletal.....	7
Bilag 4: Sagsstatistik.....	9

Indledning

Databeskyttelsesrådgiveren udgiver hermed årsrapporten for 2023.

Årsrapporten består af 2 dele:

1. Databeskyttelsesrådgiverens bemærkninger og anbefalinger er udarbejdet på baggrund af modenhedsmålingen og nøgletal, som kommunen har indberettet til databeskyttelsesrådgiveren, samt det indblik databeskyttelsesrådgiveren har fået i forbindelse med daglig sagsbehandling.
2. Bilag med modenhedsstatus, resultater for modenhedsmåling, nøgletal for kommunen og sagsstatistik fra databeskyttelsesrådgiverens kontor.

Formål:

Årsrapporten er et værktøj til kommunen, til at prioritere opgaver og ressourcer og rapportere det løbende arbejde til kommunens ledelse og politiske styringsorganer.




Databeskyttelsesrådgiveren stiller gerne op for at præsentere rapportens indhold og give perspektiver på arbejdet med databeskyttelse.

Bemærkninger og anbefalinger

Bemærkninger og anbefalinger i rapporten er databeskyttelsesrådgiverens foreslåede prioriteringer til kommunen, baseret på resultaterne i seneste modenhedsmåling, suppleret med analyse af nøgletal samt erfaringer med afholdte tilsyn og den daglige sagsbehandling.

Det er databeskyttelsesrådgiverens opgave at understøtte en god databeskyttelseskultur hos kommunen, samt at rådgive kommunen om overholdelse af de givne krav. Det er kommunens egen beslutning, hvilket ambitionsniveau der ønskes og handles efter.

Databeskyttelsesrådgiverens bemærkninger og anbefalinger

Status	Observation på baggrund af kommunens nøgletal og modenhedsmåling 2023	Vurdering	Mulige tiltag
Bemærkning	Der mangler sandsynligvis at blive udarbejdet konsekvensanalyser. Der er utilstrækkelig detaljeringsgrad og forankring af arbejdet med konsekvensanalyser (baseret på modenhedsmåling og nøgletal).		Etablere en proces, som sikrer at kommunen gennemfører konsekvensanalyser af behandlinger, hvor dette er nødvendigt. Kommunen skal sørge for at konsekvensanalyser bliver forankret i det relevante fagområde og at konsekvensanalysen indeholder en plan for evaluering og revurdering.
Bemærkning	Ikke tilstrækkelig inddragelse af databeskyttelsesrådgiveren ved konsekvensanalyser og ved anskaffelse af nye systemer.		Kommunen skal fastlægge og dokumentere hvordan og hvornår databeskyttelsesrådgiveren inddrages, afhængigt af processen der udføres.
Anbefaling	Mangel på opdateret beredskabsplan samt test af beredskabsplanen. (baseret på modenhedsmåling).		Kommunen bør udarbejde en detaljeret plan for beredskab, så der i tilfælde af uheldsmæssige driftsforstyrrelser kan blive genskabt en normal driftstilstand. Beredskabsplanen skal løbende testes, for at kontrollere at både plan og viden hos medarbejdere er tilstrækkelig

Opsummering

Det er databeskyttelsesrådgiverens opfattelse, at kommunen i hovedtræk efterlever databeskyttelsesretten.

Kommunen er nået til et niveau, hvor arbejdet med GDPR er forankret og opgaverne til dels foregår som drift.

Databeskyttelsesrådgiveren har valgt at fokusere på de prioriteringer, der vurderes vigtigst for arbejdet med at sikre overholdelse af reglerne i lovgivningen. Kommunen bør fokusere indsatsen på at sikre tærskelvurderinger for kravet om udarbejdelse af konsekvensanalyser og få udarbejdet de nødvendige konsekvensanalyser. I den forbindelse er det vigtigt, at konsekvensanalyserne er tilstrækkeligt detaljerede og forankrede i det fagområde de tilhører.

Det er påkrævet, at databeskyttelsesrådgiveren inddrages i processen med udarbejdelse af konsekvensanalyser, og også i processen med anskaffelse af nye systemer.

Det anbefales, at kommunen prioriterer en opdateret beredskabsplan og får den testet. Dette er en standard kontrol for informationssikkerhed.

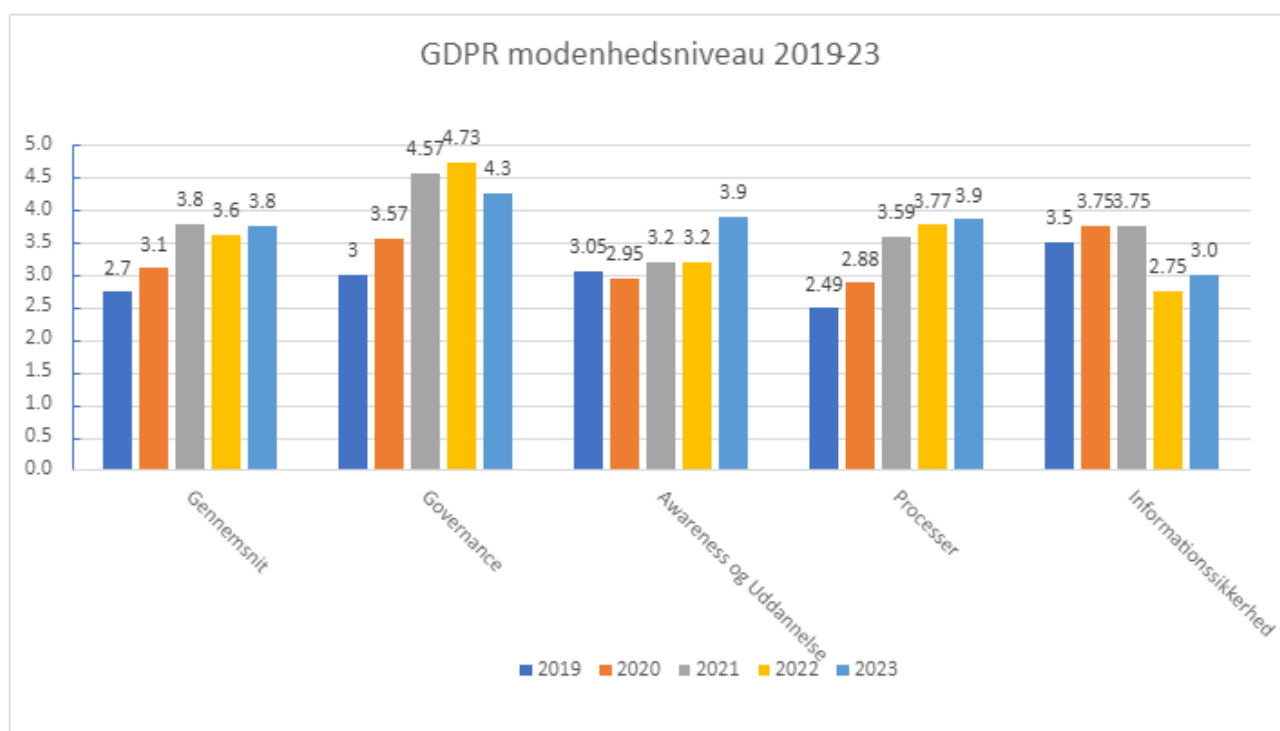
Bilag 1: Status for overholdelse af GDPR i kommunen

Databeskyttelsesrådgiveren gennemførte i november 2023 den årlige GDPR-modenhedsmåling, som måler på kommunens complianceniiveau og forudsætninger for efterlevelse af databeskyttelsesretten. Der er målt på 35 modenhedskriterier, som afspejler specifikke krav i GDPR eller på anden måde har relevans for implementering af GDPR og drift af GDPR-opgaver i kommunen.

Målingen er foretaget som selvevaluering, hvor udpegede respondenter i kommunen har afgivet individuelle besvarelser. Resultatet af disse besvarelser giver dermed en indikation for kommunens GDPR-modenhedsniveau for 2023.

Målestokken er baseret på en skala fra 1-5, som giver en indikation for overholdelse af GDPR (såkaldt GDPR-compliance). Kommunen bør som minimum stræbe efter modenhedsniveau 3 eller højere¹.

Model 1: Resultat af GDPR-modenhedsmåling i 2023 sammenlignet med målingen i 2022, 2021, 2020 og 2019



¹ Det er ikke et krav at have modenhedsniveau 5 for at overholde GDPR eller have et tilfredsstillende modenhedsniveau med undtagelse af kriterier om indgåelse af databehandlaftaler, gennemførelse af tilsyn med databehandlere samt gennemførelse af risikovurderinger for behandling, hvor niveau 5 svarer til 100 % overholdelse af GDPR.

Bilag 2: Data fra modenhedsmålingen

Nr	Spørgsmål	Emne	2022	2023
1	Direktion og ledelse understøtter GDPR-Compliance	Governance	5	5
2	Roller og ansvar	Governance	5	5
3	Databeskyttelsespolitikker	Governance	5	4
4	Opdatering af databeskyttelsespolitikker	Governance	4	4
5	Kommunikation af databeskyttelsespolitikker	Governance	5	4
6	Kendskab til kommunens databeskyttelsespolitikker	Governance	3.8	4.1
7	Monitorering af databeskyttelsespolitikker og GDPR-compliance	Governance	5	3
8	Årshjul for GDPR-arbejdsopgaver	Governance	5	5
	Gennemsnit		4.73	4.26
9	Awareness	Awareness og Uddannelse	3	4
10	Uddannelse	Awareness og Uddannelse	3.4	3.8
	Gennemsnit		3.20	3.90
11	Fortegnelse	Processer	4.2	4.3
12	Indsamling til sagligt formål og kun nødvendige personoplysninger (princippet om dataminimering)	Processer	3.6	3.7
13	Datakvalitet(princippet om rigtighed)	Processer	3.6	3.7
14	Formålsbegrænsning(princip om formålsbegrænsning)	Processer	3.8	3.7
15	Opbevaringsbegrænsning(princippet om opbevaringsbegrænsning)	Processer	3.9	3.6
16	Hjemmel til behandling	Processer	3.6	4
17	Oplysningspligt	Processer	3.7	3.9
18	Håndtering af den registreredes rettigheder	Processer	3.4	3.5
19	Klager fra registrerede	Processer	3	3
20	Håndtering af brud på persondatasikkerhed	Processer	4	4
21	Register for databehandlere	Processer	4	4
22	Kvalitetssikring af databehandleren(due dilligence)	Processer	4	3
23	Kvalitetssikring af databehandleraftaler	Processer	5	5
24	Indgåelse af databehandleraftaler	Processer	5	5
25	Procedure for tilsyn med databehandleren	Processer	5	5
26	Tilsyn med databehandlere	Processer	5	5
27	Risikovurdering efter GDPR	Processer	3	5

28	Implementering af passende sikkerhedsforanstaltninger	Processer	3	3
29	DPIA(konsekvensanalyse)/tærskelvurdering	Processer	3	3
30	Sikkerhedstest	Processer	2	2
31	Adgangsstyring til personoplysninger og systemer	Processer	3.9	4.1
32	Inddragelse af DPO	Processer	4	4
33	Privacy by design og privacy by default	Processer	3	3
	Gennemsnit		3.77	3.85
34	Sikkerhedsprogram (ISO27001)	Informationssikkerhed	3	4
35	Risikovurdering og sikkerhedsforanstaltninger (ISO27001)	Informationssikkerhed	4	4
36	Beredskabsplan	Informationssikkerhed	2	2
37	Beredskabstest	Informationssikkerhed	2	2
	Gennemsnit		2.75	3
			3.61	3.75
		Afrundet	3.6	3.8

Bilag 3: Nøgletal

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

Antal	2023
Indsigt i egne persondata	7
Begrænsning af behandling af egne persondata	- *
Berigtigelse af egne persondata	- *
Sletning af egne persondata	-*
Dataportabilitet	-*
Indsigelse mod behandling af egne persondata	0
Indsigelse mod automatiseret afgørelse, herunder profilering	0
Anmodninger behandlet inden for lofristen på 30 dage	7
Anmodninger besvaret inden for forlænget frist (maksimalt 3 måneder)	0

* Vi opgør ikke disse områder specifikt i relation til GDPR, men behandler henvendelser af denne karakter.

Brud på persondatasikkerheden

Antal	2023
Registrerede brud på persondatasikkerheden	46
Brud anmeldt til Datatilsynet	23
Brud hvoraf der er sket underretning til borgere (eller andre personer), som er genstand for bruddet	22
Anmeldelser til Datatilsynet inden for lofristen på 72 timer	23

Nye it-løsninger og inddragelse af databeskyttelsesrådgiveren

Antal	2023
Anskaffelse af nye it-løsninger til brug for behandling af persondata	11
Inddragelse af databeskyttelsesrådgiveren ved anskaffelse af nye it-løsninger til brug for behandling af persondata	6

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

Antal	2023
-------	------

Gennemførte risikovurderinger	130* sårbarhedsvurderinger 83** konsekvensvurderinger
Gennemførte tærskelvurderinger	10
Gennemførte konsekvensanalyser	
Rådføring med databeskyttelsesrådgiveren ved gennemførelse af konsekvensanalyser	

*130 sårbarhedsvurderinger på systemer er opdateret eller udarbejdet fra ny

**83 konsekvensvurderinger af behandlingsaktiviteter er opdateret eller udarbejdet på ny (der er ikke udarbejdet en egentlig DPIA i 2023)

Tilsyn/henvendelser/påtaler og bøder fra Datatilsynet

Antal	2023
Tilsyn	1
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	0
Bøder fra Datatilsynet	0

Interne kontroller i kommunen med overholdelse af GDPR

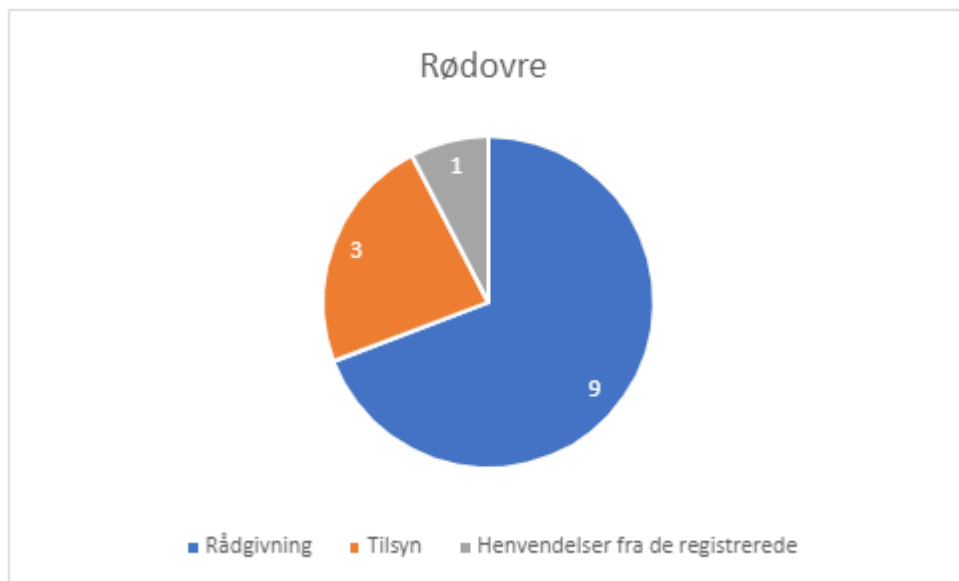
Antal	2023
Planlagte tilsyn	*
Emne for planlagt tilsyn	*
Gennemførte tilsyn	*
Emne for gennemført tilsyn	*

I år har der ikke været udført compliancetilsyn pga. andre større opgaver og udskiftning af personale.

Kommunens GDPR-ressourcer

Antal	2023
Dedikerede årsværk til implementering og drift af GDPR	2
Øvrige årsværk til implementering og drift af GDPR	6

Bilag 4: Sagsstatistik



Databeskyttelsesrådgiveren har i perioden 1. januar 2023 til og med 31. december 2023 oprettet i alt 21 sager.

Heraf er 8 sager rådgivning givet til Rødovre, som en del af Databeskyttelsesrådgiverens arbejde for alle 12 kommuner i Den Storkøbenhavnske Digitaliseringsforening.