Databeskyttelsesrådgiverens rapport 2022/2023

Rebild
KOMMUNE

Indholdsfortegnelse

Indledning 3
Kontroller og tilsyn 3
Tilsyn med databehandlere og databehandleraftaler og tilsyn med aftaler om fælles dataansvar 5
Det fælleskommunale Databehandlersekretariat 5
Databehandleraftaler med de mindre leverandører, som ikke omfattes af DBS 5
Tilsyn med aftaler om fælles dataansvar ..... 6~~5~~
Anbefaling 6
Brugerrettigheder og logning 6
Iværksættelse 6
Anbefaling 6
Sikkerhedsbrud og sikkerhedshændelser 7
Antal sikkerhedsbrud 7
Læring og iværksættelse af tiltag 7
Awareness, samt måling af medarbejdernes generelle vidensniveau om informationssikkerhed og overholdelse af databeskyttelsesreglerne 7
Anbefaling 8
Sletning 8
Projekt Datarejsen 8
Anbefaling 9
Fortegnelserne 9
Risikovurderinger og konsekvensanalyser (DPIA) 9
Opfølgning på Privacy by Design 10
Opdatering af trusselsbilledet og mulige forbedringer 10
Tilsyn med udført it-revision 10
Revision af informationssikkerhedspolitik, samt it-sikkerhedshåndbog 11
Anbefaling 11
Særlige emner 11
Tilsyn fra Datatilsynet – oktober 2022 11
Datatilsynets fem konkrete anbefalinger: 12
Datatilsynets undersøgelse vedrørende DPO – marts 2023 13
Konklusion og anbefalinger 14
Anbefalinger 14

Indledning

Denne rapport er udarbejdet af Rebild Kommunes DPO, med henblik på at informere kommunens øverste ledelse om status på Rebild Kommunes implementering og overholdelse af databeskyttelsesreglerne - som fastlagt i EU-Databeskyttelsesforordningen (GDPR) (EU 2016/679), samt i de danske vedtagne bestemmelser om samme (Databeskyttelsesloven nr. 502 af 23/05/2018).

DPO'en er uvildig, må ikke modtage instruktion i udførelse af sine arbejdsopgaver, og rapporterer direkte til øverste ledelsesniveau. Evaluering og afrapportering af status sker i løbet af året, løbende til kommunens informationssikkerhedsudvalg, samt én gang årligt ved aflæggelse af denne rapport til byrådet.

I det følgende vil blive gennemgået områder af betydning for Rebild Kommunes efterlevelse af gældende bestemmelser på databeskyttelsesområdet. Rapporten afsluttes med DPO's status og vurdering af Rebild Kommunes overholdelse af reglerne, samt anbefalinger til det fortsatte implementeringsarbejde.

Kontroller og tilsyn

DPO'en skal, som en del af overvågningsopgaverne indsamle oplysninger, der identificerer databehandlingsaktiviteter, og analysere og kontrollere databehandlingsaktiviteternes overholdelse af bestemmelserne.

DPO'en har tillige til opgave at overvåge organisationens overholdelse af implementerede interne politikker.

For at føre tilsyn med, at forvaltningen efterlever databeskyttelsesreglerne på betryggende vis, gennemføres en række kontrolaktiviteter løbende år efter år, mens andre er fritstående aktiviteter. Fritstående kontrolaktiviteter udvælges på baggrund af aktualitet og risikovurderinger.

Aktiviteter, der gentages, er placeret i årshjulet med det formål at illustrere årets aktiviteter simpelt og overskueligt. Fritstående aktiviteter, der kan variere hen over årene, beskrives i en årsplan, der udarbejdes én gang om året.

I det følgende vil blive gennemgået udvalgte kontrolområder og DPO's resultater af tilsynet. Rapporterne, samt relevant dokumentation for de løbende kontroller, er journaliseret i kommunens dokumenthåndteringssystem, SbSys.

I rapporten er inkluderet resultater fra kontrolrapporter for perioden 1. november 2022 -31. august 2023.

Årshjul med løbende kontroller

Tilsyn med databehandlere og databehandleraftaler og tilsyn med aftaler om fælles dataansvar

Forvaltningen skal udarbejde databehandleraftaler med databehandlere, samt føre tilsyn med disse. DPO fører tilsyn med, at forvaltningen har lagt en plan for tilsyn, samt følger planen. DPO fører ligeledes tilsyn med, at forvaltningens tilsyn med databehandlere og databehandleraftaler omfangsmæssigt er tilstrækkeligt, samt at tilsynet sker tilstrækkeligt ofte ud fra en risikobaseret vurdering af behovet.

Det fælleskommunale Databehandlersekretariat

KL tog i 2020 initiativ til et tværfagligt samarbejde om at føre tilsyn med databehandleraftaler, som går på tværs af landets kommuner. Til dannelse af samarbejdet oprettes foreningen Det fælleskommunale databehandlersekretariat (DBS). Rebild Kommune har tilsluttet sig dette samarbejde. Sekretariatet fører tilsyn med databehandlere, der benyttes af sammenlagt flere end 20 af de tilsluttede kommuner.

DBS oplyser i deres nyhedsbrev af februar 2023:

"*Som anført har DBS nu publiceret en række tilsynsrapporter. Aktuelt har vi publiceret tilsynsrapporter vedrørende mere end 200 systemer og herudover er vi i gang med tilsyn på mere end 100 systemer. Vi sætter nu også gang i tilsyn med systemer fra Microsoft, KOMBIT og KMD, og vi har holdt møder med repræsentanter fra de tre store leverandører. På møderne har vi drøftet rammer og processer for tilsynene*"

Databehandlersekretariatets tilsyn med databehandlere, omfattet af aftalen med sekretariatet, ses altså behørigt iværksat.

Databehandleraftaler med leverandører, som ikke omfattes af DBS

Rebild Kommune har indtil nu ikke haft ressourcer til at føre tilsyn med databehandleraftaler, der ikke er omfattet af medlemskabet i DBS. Det drejer sig om 109 databehandleraftaler, ud af de i alt 217 aftaler, Rebild kommune på nuværende tidspunkt har indgået. I forbindelse med anbefalinger i DPO's afrapportering for 2021-22, har forvaltningen responderet ved at lægge en plan for tilsyn med de leverandører, som ikke omfattes af DBS.

Det oplystes primo 2023 fra Fællescenter Sekretariat (it-afdelingen):

"*DPO's anbefaling omhandler de mindre databehandleraftaler, hvor der er færre end 20 kommuner, der anvender systemerne. Tilsynet med disse er indarbejdet i it-sikkerhedsteamets årsplan 2023 og forventningen er, at anbefalingen herved kan imødekommes*"

Opdatering 1. august 2023:

En opdatering fra informationssikkerhedsteamet viser dog, at man har været nødt til at opprioritere andre complianceopgaver, og at tilsynet med databehandleraftaler der ikke er omfattet af DBS derfor igen er nødtvungent nedprioriteret for 2023.

Tilsyn med aftaler om fælles dataansvar

Rebild Kommune har ikke indgået nogen aftaler om fælles dataansvar.

Anbefaling

Det anbefales på det kraftigste, at der snarest iværksættes løbende og regelmæssigt tilsyn med de databehandlere og databehandleraftaler, der ikke omfattes af Databehandlersekretariatets tilsyn. Det er kritisabelt, at der ikke konsekvent og struktureret har været ført tilsyn med disse databehandleraftaler siden 2020.

DPO anbefalede i 2018, at kontrol- og tilsynsområdet fik tilført ressourcer, idet opgaven med at føre tilsyn er ressourcetung. I såvel 2021 som 2022 anbefalede DPO, at der iværksattes løbende og regelmæssigt tilsyn, og i 2022 nåede anbefalingen toppen af listen over anbefalinger, idet DPO vurderede, at det manglende tilsyn med databehandlere, der ikke er omfattet af DBS, burde have højeste prioritet.

At tilsynet endnu et år er blevet nedprioriteret er kritisabelt, og det skal på det kraftigste anbefales, at der lægges en snarlig plan for, hvordan Rebild Kommune vil finde ressourcer til at løse opgaven i det kommende år.

Brugerrettigheder og logning

Der er ført tilsyn med, om forvaltningen har foretaget jævnlig gennemgang af brugerrettigheder til systemer med personoplysninger og logning af adgang til de samme.

Der skal blandt andet følges op på, om fratrådte medarbejderes adgange er lukkede, og om der er behov for ændringer i adgangsforhold, hvis en eller flere medarbejdere for eksempel har skiftet arbejdsopgaver/funktion mv. Desuden skal kontrolleres, om adgangen er for vid; Har flere medarbejdere end nødvendigt adgang til de samme sager?

For systemer, der behandler følsomme eller fortrolige personoplysninger, skal der løbende ske opfølgning på eventuelle afviste loginforsøg. Dertil skal der ske stikprøvegennemgang af loggen i forhold til hvem, der har behandlet personoplysninger i en sag, og hvorvidt denne behandling har været sagligt begrundet.

Iværksættelse

Det oplyses af informationssikkerhedsteamet, at opgaven for så vidt angår systemer med decentral brugeradministration er lagt ud til system- og dataejerne (centercheferne), men at de har brug for konkret støtte og vejledning i forhold til tilrettelæggelse af brugeradgangskontrol og logning. Støtte og vejledning vil blive givet som facilitering af workshops i centrene. Disse workshops er endnu ikke skemalagt, men vil blive afholdt efteråret 2023.

Der er på nuværende tidspunkt udarbejdet detaljerede procesbeskrivelser og retningslinjer til forvaltningen, godkendt af informationssikkerhedsudvalget juni 2023, og disse vil blive præsenteret for systemejerne på de nævnte workshops.

Anbefaling

Det anbefales på det kraftigste, at kommunen retter op på efterslæbet med at etablere en systematisk og struktureret procedure for jævnlig kontrol af brugeradgange og logning. Arbejdet bør prioriteres og iværksættes snarest. Det er kritisabelt, at Rebild Kommune 5 år efter GDPR's ikrafttræden endnu ikke konsekvent og struktureret har tilrettelagt og gennemført kontrol på området.

Denne anbefaling bifaldes af Datatilsynet, som i deres tilsyn ultimo 2022, netop angiver dette som én af deres 5 konkrete anbefalinger til Rebild Kommune.

Også årets it-revision er mundet ud i minimum 4 anbefalinger af relevans for kontrollen af brugerrettigheder og logning. Der er altså tale om et emne med stort fokus, men aktuel ringe efterlevelse i Rebild Kommune.

Sikkerhedsbrud og sikkerhedshændelser

Der skal føres tilsyn med, at forvaltningen håndterer og lærer af hændelser og sikkerhedsbrud. Ud fra loggen over hændelser følges der op på, hvilken type hændelser og sikkerhedsbrud der er sket i perioden - omfang, type, konsekvens. Herunder status på udbedring og forebyggende foranstaltninger. Er der besluttet forebyggende foranstaltninger, og har forvaltningen planlagt behørige ændringer til forebyggelse af lignende hændelser og sikkerhedsbrud?

Kommunens nedsatte informationssikkerhedsudvalg orienteres på et fast dagsordenpunkt om de senest indkomne sikkerhedsbrud. Dette sker blandt andet med henblik på jævnlig opfølgning af antallet af og typen af sikkerhedsbrud, samt hvilke tiltag der bør sættes i værk for at forebygge lignende typer sikkerhedsbrud fremover. DPO deltager på disse møder, og det er vurderingen, at informationssikkerhedsudvalget behørigt forholder sig til eventuelle behov for forebyggende tiltag.

Antal sikkerhedsbrud

I perioden 1. november 2022 – 31. august 2023 er der registreret i alt 36 sikkerhedsbrud. 13 af disse er anmeldt til Datatilsynet. Niveauet afviger ikke stort fra sidste års antal sikkerhedsbrud. Niveauet skiller sig heller ikke ekstremt ud fra andre sammenlignelige kommuner, omend det kan være meget svært at sammenligne, idet praksis for håndteringen af sikkerhedsbrud adskiller sig fra kommune til kommune.

Læring og iværksættelse af tiltag

Siden seneste rapport er det besluttet at indføre ny procedure i forbindelse med sikkerhedsbrud. Informationssikkerhedsudvalget har 13. marts 2023 besluttet, at centerchefer fremadrettet altid underrettes om sikkerhedsbrud i eget center. Formålet er at opnå ekstra læring og dermed kvalificere grundlaget for opfølgning på eksisterende procedurer.

Rebild Kommune iværksætter i efteråret 2023 en GDPR- og cybersikkerhedskampagne. Awarenesskampagnen vil forhåbentlig bidrage til en større viden i organisationen om sikkerhedsbrud, men vil muligvis også afføde en større mængde indberetninger af sikkerhedsbrud til informationssikkerhedsteamet. Dette vil næste års rapport kunne afsløre.

Awareness, samt måling af medarbejdernes generelle vidensniveau om informationssikkerhed og overholdelse af databeskyttelsesreglerne

Der er fulgt op på, at Rebild Kommune løbende afholder awareness for medarbejderne, ligesom der er fulgt op på, at der jævnligt foretages målinger af medarbejdernes generelle vidensniveau om GDPR.

Rebild Kommune gennemførte ultimo 2018 en GDPR-awarenesskampagne i form af et e-learningskursus. Kurset blev efterfølgende lagt på Rebild Kommunes intranet, således nye og gamle medarbejdere kunne tilgå det. Grundet skift af it-udbyder, blev kurset taget ned, og der har ikke siden været adgang til decideret e-learning eller andre former for regelmæssige kurser om GDPR.

Tidligere år har it-afdelingen årligt haft tilbagevendende drøftelser med systemansvarlige centerchefer, hvorunder også blev inddraget drøftelser om GDPR og informationssikkerhed. Dette gav informationssikkerhedskoordinator og it-chef et overordnet overblik over den generelle viden om GDPR i forvaltningen.

Disse årligt tilbagevendende drøftelser har dog ikke været gennemført de seneste år, og der er ikke foretaget nogen egentlige målinger af medarbejdernes generelle vidensniveau om GDPR og informationssikkerhed.

Ved kontrollerne i både 2020 og 2021 blev det oplyst, at forvaltningen agtede at bruge flere ressourcer og iværksætte awareness for medarbejderne. I november 2022 oplystes det videre, at der var forhandlinger i gang med virksomhed, der udbyder GDPR som e-learning, og at indkøb af e-learning var godkendt til starten af 2023.

Iværksættelse af den planlagte e-learning ses endnu ikke konkret iværksat. Det oplyses, at systemet er indkøbt, og at der kun mangler få detaljer, samt en godkendelse fra direktionen, før kurset kan rulles ud til medarbejdere og ledere i kommunen.

Anbefaling

Grundet den meget lange periode uden konkret og struktureret adgang til kursusmateriale om GDPR, anbefales det på det kraftigste, at den indkøbte e-learning udrulles snarest.

Sletning

DPO kontrollerer, at kommunen har tilrettelagt sin myndighedsopgave således, at databeskyttelsesbestemmelserne om sletning overholdes.

Når det ikke længere er nødvendigt at behandle personoplysninger, skal de slettes. Personoplysninger skal opbevares på en sådan måde, at det ikke er muligt at identificere de registrerede i et længere tidsrum end det, der er nødvendigt til de formål, hvortil de pågældende personoplysninger behandles. Det samme gælder, hvis en borger ønsker, at oplysninger om denne skal slettes. Det betyder blandt andet, at alle systemer til behandling af personoplysninger – eg. elektroniske journalsystemer og fagsystemer – skal indstilles til at slette personoplysninger og personsager i henhold til reglerne for de enkelte fagområder.

Projekt Datarejsen

Rebild Kommune igangsatte i 2021 projektet "Datarejsen" med henblik på at skabe et overblik over dataflow og datahåndtering i alle dele af forvaltningen. En essentiel del af Datarejsens formål er også sikring af forvaltningens persondatahåndtering i forbindelse med lovkravene til sletning.

Datarejsen kørte fortløbende i 2022, og i 2023 oplystes, at der er udarbejdet og afrapporteret datakvalitetsrapporter for Center Arbejdsmarked og Borgerservice, Center Familie og Handicap, Center Sundhed Kultur og Fritid, samt Center Pleje og Omsorg. Datarejsen er igangsat i Center Natur og Miljø og Center Plan, Byg og Vej, og der er indkaldt til opstartsmøde i Fællescenter Sekretariat og Fællescenter Økonomi samt Center Børn og Unge senere på året.

Det oplyses dog af informationssikkerhedsteamets repræsentant i Datarejsen, at anbefalinger vedrørende emnet sletning vil blive implementeret særskilt og i forbindelse med kommende workshops i centrene. Disse workshops er endnu ikke skemalagt, men vil blive afholdt efteråret 2023.

Der er på nuværende tidspunkt udarbejdet grundige og detaljerede vejledninger til forvaltningen, og disse vil blive præsenteret og implementeret for systemejerne på de nævnte workshops.

Anbefaling

DPO har i alle afrapporteringer siden 2019 anbefalet iværksættelse af tiltag, der bevirker, at Rebild Kommune kan blive lovmedholdelig på området for behørig sletning af borgernes persondata. Dette ses endnu ikke at være sket, og det anbefales på det kraftigste, at kommunen retter op på efterslæbet. Det er kritisabelt, at Rebild Kommune 5 år efter GDPR's ikrafttræden endnu ikke har sikret behørig sletning af de registreredes persondata.

Fortegnelserne

Der skal føres tilsyn med, at forvaltningen behørigt fører og opdaterer fortegnelserne over behandlingsaktiviteter. Har kommunen udarbejdet fortegnelser for samtlige behandlingsaktiviteter, og er de retvisende? Kontrolleres det løbende, at fortegnelserne er retvisende, og er der procedurer, som sikrer, at der udarbejdes nye fortegnelser/sker tilpasning af eksisterende, når der startes nye behandlingsaktiviteter?

Det bekræftes, at forvaltningen behørigt fører fortegnelser over behandlingsaktiviteter. Det oplyses dog også, at der er planlagt en opdatering af måden, fortegnelserne udarbejdes og håndteres på, men at denne opdatering først vil ske i 2024.

Det vurderes, at fortegnelserne på nuværende tidspunkt holder en minimumsstandard, der opfylder kravene i databeskyttelsesbestemmelserne. Det anbefales dog, at en opdatering af kommunens fortegnelser ikke udskydes til senere end 2024.

Risikovurderinger og konsekvensanalyser (DPIA)

En dataansvarlig skal, når der behandles personoplysninger, gennemføre passende tekniske og organisatoriske foranstaltninger for at sikre, og for at være i stand til at påvise, at behandlingen er i overensstemmelse med databeskyttelsesforordningen. Den dataansvarlige skal i den forbindelse vurdere, hvilke negative konsekvenser en behandling vil kunne få for den registrerede. En konsekvensanalyse skal herefter udarbejdes, når en behandling sandsynligvis vil medføre en høj risiko for den registreredes rettigheder og frihedsrettigheder.

"Hvis en type behandling, navnlig ved brug af nye teknologier og i medfør af sin karakter, omfang sammenhæng og formål, sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder, foretager den dataansvarlige forud for behandlingen en analyse af de påtænkte behandlingsaktiviteters konsekvenser for beskyttelse af personoplysninger."

DPO skal inddrages og rådføres, når der foretages en konsekvensanalyse.

Der er i den forgangne periode foretaget konsekvensanalyse af Google Workspace, og DPO har været behørigt inddraget i arbejdet.

Der ses dog også behov for konsekvensanalyser af visse eksisterende systemer. Blandt andet kan Aula, KSD og KL Gateway, i medfør af sin karakter, medføre en høj risiko for enkeltpersoners rettigheder og frihedsrettigheder.

Datatilsynet gennemførte ultimo 2022 et skriftligt tilsyn af Rebild Kommune og 54 andre kommuner og regioner. På baggrund af tilsynet tildeltes Rebild Kommune fem anbefalinger af Datatilsynet. En af de fem anbefalinger lød på et øget fokus på udarbejdelse af konsekvensanalyser.

Informationssikkerhedsteamet oplyser dog, at udarbejdelsen af konsekvensanalyser pt. er nedprioriteret på grund af et opprioriteret fokus på udarbejdelse af sikkerhedsregler, awareness, tilsyn fra DBS mm.

Det anbefales, at der afsættes tid og ressourcer til et øget fokus på udarbejdelse af risikovurderinger og konsekvensanalyser i det omfang det er relevant.

Opfølgning på Privacy by Design

Databeskyttelse gennem design indebærer ifølge databeskyttelsesforordningen, at den dataansvarlige allerede fra tidspunktet, hvor midlerne for behandlingen fastlægges (for eksempel et nyt IT-system), skal gennemføre passende tekniske og organisatoriske foranstaltninger, som er designet med henblik på at sikre en effektiv implementering af de grundlæggende databeskyttelsesprincipper, det er for eksempel lovlighed, rimelighed og gennemsigtighed.

Kort sagt skal den dataansvarlige på forhånd have designet og indrettet sin it-mæssige og organisatoriske forretningsunderstøttelse af behandlinger sådan, at forordningens krav og beskyttelseshensyn varetages som en integreret del i hele behandlingsforløbet.

I Rebild Kommune bliver Privacy by Design sikret ved påtænkte nyanskaffelser, blandt andet ved at holde systemet op imod en udarbejdet tjekliste. Også den benyttede standarddatabehandlerskabelon sikrer, at Privacy by Design naturligt tænkes ind ved nyanskaffelser. Endeligt indgår Privacy by Design som en naturlig bestanddel af projekt Datarejsen, som er en helhedsorienteret indsats iværksat for at skabe klare rammer for kommunens datahåndtering i alle dele af opgaveløsningen.

Opdatering af trusselsbilledet og mulige forbedringer

Der er ført tilsyn med, at forvaltningen har forholdt sig til det aktuelle trusselsbillede og risikovurderet på, om eventuelle forbedringer skal iværksættes, jf. artikel 32, stk. 1, i databeskyttelsesforordningen.

Hele it-afdelingen er inddraget i den løbende opgave med at holde øje med trusselsbilledet. I det daglige arbejde modtager it-afdelingens ansatte en god viden om aktuelle it-trusler via såvel indmeldinger fra kommunens medarbejdere, som nyhedsbreve, netværksgrupper og overordnede myndigheder. Især Center for Cybersikkerhed sørger for at fodre kommunerne med vigtig viden på området.

CFCS hævede maj 2023 trusselsniveauet fra cyberaktivisme til HØJ, mens de øvrige trusselsniveauer er uændrede. CFCS vurderer altså fortsat, at truslen fra cyberspionage og cyberkriminalitet er MEGET HØJ, hvorimod truslen fra destruktive cyberangreb er LAV, og truslen for cyberterror er INGEN. Rebild Kommune holder sig opdateret og oplyser, at de handler på baggrund af det opjusterede trusselsniveau. Blandt andet er der indkøbt e-learning om cybersikkerhed til hele organisationen, og kurset forventes udrullet efteråret 2023.

Tilsyn med udført it-revision

DPO har ført tilsyn med, at der udføres it-revision, samt at forvaltningen samler op på og retter ind efter revisionens anbefalinger i forhold til informationssikkerhed og databeskyttelsesreglerne.

Kommunens revisor, BDO, har i marts 2023, som et led i den samlede revision af årsregnskabet for 2022, udført it-revision i Rebild Kommune.

Revisionen oplyser i deres opsummering:

"Det er vores opfattelse, at kommunen i alle væsentlige henseender har implementeret hensigtsmæssige interne it-kontroller, der medvirker til at opretholde informationernes integritet og sikkerheden af data, som it-systemerne behandler i forhold til regnskabsføringen og regnskabsaflæggelsen"

Revisionen har dog konstateret mangler i kommunens forretningsgange og interne kontroller, og har angivet et antal anbefalinger til gennemførelse. Anbefalingerne er prioriteret fra 1-3, hvor 1 er højeste prioritet. Sondringen mellem de enkelte prioriteringer er sket ud fra en faglig vurdering af kommunens it-sikkerhedshåndtering sammenholdt med begrebet god it-skik, herunder en vurdering af væsentlighed og risiko. Der ses oplyst i alt syv prioritet 2-anbefalinger, samt en enkelt prioritet 3-anbefaling. Der ses i år ingen prioritet 1-anbefalinger. Der ses videre, at forvaltningen har taget stilling til såvel tidligere anbefalinger fra revisionen, som aktuelle. Det vurderes, at forvaltningen retter behørigt ind, hvor nødvendigt.

Revision af informationssikkerhedspolitik, samt it-sikkerhedshåndbog

Ifølge databeskyttelsesforordningens artikel 32, stk. 1, skal der føres tilsyn med, at forvaltningen har truffet beslutning om, og implementeret, en informationssikkerhedspolitik. På samme måde skal der føres tilsyn med, at forvaltningen har udarbejdet en it-sikkerhedshåndbog; at der er udarbejdet skriftlige retningslinjer for den ønskede brugeradfærd blandt medarbejdere ved brug af it-udstyr, devises, e-mail, relevante programmer mv.

Der skal ligeledes føres tilsyn med, at kommunen forholder sig til, hvorvidt begge fortsat er dækkende eller skal revideres.

Det fremgik af Rebild Kommunes intranet, at der blev udarbejdet en it-sikkerhedspolitik for hele kommunen i 2013 – revideret februar 2017. Der blev udarbejdet et udkast til informationssikkerhedspolitik november 2021. Informationssikkerhedspolitikken ses godkendt af byrådet den 28. april 2022.

Det ses, at der er i 2023, er ved at blive udarbejdet en opdateret udgave af it-sikkerhedshåndbogen. Dette arbejde følges tæt.

Anbefaling

DPO anbefalede i rapporterne for såvel 2019, som for 2020 og 2021 og 2022, at der foretoges en opdatering af sikkerhedshåndbogen. Det anbefales, at det iværksatte initiativ med opdatering af it-sikkerhedshåndbogen, fortsættes og færdiggøres i snar fremtid.

Særlige emner

Tilsyn fra Datatilsynet – oktober 2022

Rebild Kommune blev den 30. august 2022, sammen med 54 andre kommuner og regioner, udtaget til et skriftligt tilsyn af Datatilsynet, som undersøger kommunens modenhed på GDPR-området. Tilsynet blev gennemført som et skriftligt tilsyn i form af en række spørgsmål.

Tilsynene har baggrund i Datatilsynets strategi om en mere data- og risikobaseret tilgang til vejledning og kontrol. Formålet med tilsynene var blandt andet, at Datatilsynet skal kunne foretage en overordnet vurdering af forskellige organisationers modenhed i forhold til databeskyttelse. Tilsynene tog udgangspunkt i en sammenligning af besvarelserne på tværs af ensartede dataansvarlige.

Tilsynet mundede i december 2022 ud i en rapport indeholdende grafer, der illustrerer centrale tal fra tilsynets modenhedsanalyse vedrørende Rebild Kommune og tilsvarende organisationer. I rapporten er

benchmarking udført på den måde, at der sammenlignes på tværs af besvarelser fra lignende organisationer (kommuner over for kommuner og regioner over for regioner). Hensigten er at give Rebild Kommune mulighed for at vurdere eget modenhedsniveau i forhold til det gennemsnitlige modenhedsniveau for sammenlignelige organisationer.

Rapporten indeholder ligeledes fem konkrete anbefalinger, som Datatilsynet, blandt andet på baggrund af besvarelsen, vurderer er særligt relevante for det videre arbejde med persondatasikkerhed i Rebild Kommune. Anbefalingerne er valgt ud fra en samlet, overordnet vurdering af Rebild Kommunes besvarelse.

Datatilsynets fem konkrete anbefalinger:

- **Periodisk kontrol af adgangsrettigheder -** For at undgå utilsigtede adgange til personoplysninger, bør Rebild Kommune have fokus på styring af brugeres adgangsrettigheder. Fejl i rettighedsstyring kan for eksempel opstå via brugerfejl (for eksempel kopiering af eksisterende adgangsrettigheder ved nyoprettelse) og pga. manglende handling, (for eksempel manglende opdatering af rettigheder ved ændringer i organisationen).

- **Scanning af mail** - Ved hyppig brug af e-mail til fremsendelse af personoplysninger vil der være en øget risiko for utilsigtet videregivelse af oplysninger til en forkert part. Der er også mulighed for, at personoplysninger overses, fordi de er skjult i meta-data, eller at brugeren tror, at personoplysninger er slettet eller pseudonymiseret, selv om det ikke er tilfældet, for eksempel i forbindelse med aktindsigt. For at mindske sandsynligheden for utilsigtet videregivelse, kan organisationen scanne alle udgående e-mails for for eksempel personnumre eller andre personoplysninger, hvis format er genkendeligt, og som normalt kan forekomme i mails fra organisationen.

- **Konsekvensanalyse –** Kommuner og regioner er dataansvarlige for en række behandlingsaktiviteter, hvor der potentielt kan være en høj risiko for de registrerede. Den type af behandlingsaktiviteter kan give anledning til, at der skal udarbejdes en konsekvensanalyse for de registreredes rettigheder. Det ser ud til, at der generelt arbejdes med de risikovurderinger i organisationerne, som forudsættes efter databeskyttelsesforordningens artikel 32, men samtidig er der indikationer på, at mange organisationer ikke er nået lige så langt i arbejdet med konsekvensanalyser efter databeskyttelsesforordningens artikel 36. Det kan betyde, at der sker behandlinger, hvor risikoen for de registrerede ikke er tilstrækkeligt adresseret.

- **Flerfaktorautentifikation** – For at undgå uautoriseret adgang til personoplysninger og angreb, som for eksempel ransomwareangreb, skal login, som er tilgængeligt fra internettet, (eventuelt også interne login) være styrket med flerfaktorautentifikation. Det er desværre relativt udbredt, at medarbejdere genbruger passwords flere steder, herunder også det password, som medarbejderne bruger til at logge på arbejdskontoen. Derfor kan et login, der kun er baseret på dette password, være sårbart. En velvalgt, yderligere login-faktor kan sænke sandsynligheden for misbrug betydeligt.

- **Domænesikkerhed** - For at undgå, at organisationens hjemmesider eller mailadresser bliver brugt til it-kriminalitet, er der nogle anbefalinger vedrørende domænesikkerhed, som Rebild Kommune kan følge.

Datatilsynets undersøgelse vedrørende DPO – marts 2023

Datatilsynet henvendte sig 21. marts 2023 med en undersøgelse vedrørende anvendelsen af databeskyttelsesrådgivere. Undersøgelsen er en del af en koordineret undersøgelse fra Det Europæiske Databeskyttelsesråd (EDPB).

I Danmark har Datatilsynet valgt at afgrænse undersøgelsen til at omfatte de databeskyttelsesrådgivere, der er udpeget for landets kommuner. Baggrunden herfor er blandt andet, at kommunerne efter databeskyttelsesforordningen er forpligtet til at udpege en databeskyttelsesrådgiver, samt at kommunerne i høj grad beskæftiger sig med borgerrelateret arbejde, som indebærer behandling af store mængder personoplysninger.

Formålet med undersøgelsen er at skabe et overblik over databeskyttelsesrådgivernes arbejde og eventuelle udfordringer forbundet hermed. Resultatet af undersøgelsen vil blive samlet i en national rapport, hvor Datatilsynet vil evaluere behovet for mere konkret vejledning. Herudover vil undersøgelsen blive anvendt i en samlet EDPB-rapport i aggregeret form. Desuden bemærker Datatilsynet, at det ikke kan udelukkes, at undersøgelsen kan danne grundlag for iværksættelse af konkrete tilsyn.

Resultaterne af undersøgelsen afventes.

Konklusion og anbefalinger

Det ses, at Rebild Kommune overordnet set har et relativt højt modenhedsniveau i forhold til databeskyttelsesrettens krav. Der ses dog fortsat områder, hvor kommunen endnu ikke lever op til et tilfredsstillende niveau. Disse vil i det følgende blive gennemgået og anbefalinger vil blive givet.

Anbefalingerne er angivet i prioriteret rækkefølge.

Anbefalinger

- **Tilsyn med databehandleraftaler, der ikke omfattes af aftalen med Databehandlersekretariatet -** Det anbefales på det kraftigste, at der snarest iværksættes løbende og regelmæssigt tilsyn med de databehandlere og databehandleraftaler, der ikke omfattes af Databehandlersekretariatets tilsyn.

  DPO anbefalede i 2018, at kontrol- og tilsynsområdet fik tilført ressourcer, idet opgaven med at føre tilsyn er ressourcetung. I såvel 2021 som 2022 anbefalede DPO, at der iværksattes løbende og regelmæssigt tilsyn, og i 2022 nåede anbefalingen toppen af listen over anbefalinger, idet DPO vurderede, at det manglende tilsyn burde have højeste prioritet.

  At tilsynet endnu et år er blevet nedprioriteret er kritisabelt, og det skal på det kraftigste anbefales, at der lægges en snarlig plan for, hvordan Rebild Kommune vil finde ressourcer til at løse opgaven.

- **Sletning** - DPO har i alle afrapporteringer siden 2019 anbefalet iværksættelse af tiltag, der bevirker, at Rebild Kommune kan blive lovmedholdelig på området for behørig sletning af borgernes persondata. Dette ses endnu ikke at være sket, og det anbefales på det kraftigste, at kommunen retter op på efterslæbet.

  Det er kritisabelt, at Rebild Kommune 5 år efter GDPR's ikrafttræden endnu ikke har sikret behørig sletning af de registreredes persondata.

- **Brugerrettigheder og logning** - Det anbefales på det kraftigste, at kommunen retter op på efterslæbet med at etablere en systematisk og struktureret procedure for jævnlig kontrol af brugeradgange og logning. Arbejdet bør prioriteres, og iværksættes snarest.

  Denne anbefaling bifaldes af Datatilsynet, som i deres tilsyn ultimo 2022, netop angiver dette som én af deres 5 konkrete anbefalinger til Rebild Kommune.

  Også årets it-revision er mundet ud i minimum 4 anbefalinger af relevans for kontrollen af brugerrettigheder og logning. Der er altså tale om et emne med stort fokus, men aktuel ringe efterlevelse i Rebild Kommune.

- **Awareness** - Grundet den meget lange periode uden konkret og struktureret adgang til kursusmateriale om GDPR anbefales det på det kraftigste, at den indkøbte e-learning udrulles snarest.

- **It-sikkerhedshåndbog** – DPO anbefalede i rapporterne for såvel 2019, som for 2020, 2021 og 2022, at der foretoges en opdatering af sikkerhedshåndbogen. Det anbefales, at det i 2023 iværksatte initiativ med opdatering af it-sikkerhedshåndbogen, fortsættes og færdiggøres i snar fremtid.

Det er DPO's vurdering, at der på nuværende tidspunkt ikke er iværksat tilstrækkelige organisatoriske foranstaltninger til implementering af nødvendige tiltag og efterlevelse af gældende databeskyttelsesregler. Som angivet i konklusionen herover ses efterslæb på konkrete udpegede områder, og der vil skulle iværksættes specifikke tiltag for at blive compliant.

Det er dog DPO's forventning, at Rebild Kommune med den rette mængde ressourcer og en tilpasset indsats, vil kunne rette op på de nævnte mangler.

Eva Helene Antonsen
DPO, Rebild Kommune
august 2023