Region Hovedstaden
Center for Politik og Kommunikation

DPO-rapport til Regionsrådet

Databeskyttelsesrådgiverens rapportering 2020

Indledning

Formålet med denne rapport er at rapportere om databeskyttelsesrådgiverens (DPO'ens) arbejde til og med 2020. Rapporten beskriver DPO'ens funktion, arbejdsopgaver herunder en opsamling på overvågningsdelen inkl. anbefalinger og rådgivning givet i forbindelse med 10 planlagte tilsyn udført i 2019 og efterbehandlet i 2020.

Den 25. maj 2018 trådte et nyt regelsæt på databeskyttelsesområdet i kraft. Region Hovedstaden har arbejdet intenst med reglerne siden, og har i perioden etableret en struktur for arbejdet med databeskyttelse via vejledninger i regionen, som er et vigtigt afsæt for fremtidige initiativer på området samt den daglige håndtering af person- og sundhedsoplysninger i regionen.

DPO-funktionen favner alle databehandlinger i Region Hovedstaden. Der er selvsagt stor fokus på sundhedsoplysningerne, og hovedparten af regionens databehandlinger er reguleret af både databeskyttelsesloven og sundhedsloven. Dertil kommer, at databeskyttelse er en menneskeret. Patienterne har derfor på en og samme tid både ret til sundhedsbehandling og beskyttelse af deres personoplysninger. Dette betyder også, at håndteringen af oplysningerne hurtigt bliver en kompleks affære ikke mindst, når dette kombineres med ny teknologi, krav til nye behandlingsmetoder samt nye muligheder indenfor forskning. Dette medfører også nye måder at få godkendelser på, at vurderingerne skal være grundigere, og at der er større krav til oplyst grundlag og dokumentation.

Adgang til data og personoplysninger er en nødvendighed for de fleste af regionens opgaver - ikke mindst i forbindelse med patientbehandling og forskning. Et korrekt og lovligt datagrundlag er helt essentielt for at udføre opgaverne, og derfor bliver databeskyttelse i sidste ende også en del af den gode patientbehandling, forskning og kvalitetsudvikling.

Beskrivelse af DPO-funktionen

DPO-funktionen består af DPO'en og to DPO-konsulenter. DPO'en har i hele perioden været Birgitte Hagelskjær Nielsen. I løbet af perioden har der i forhold til bemandingen været udskiftning af begge DPO-konsulenter. De to DPO-konsulenter er på rapporteringstidspunktet Magnus Sternest Andersen og Christine Boiden Søtofte. Magnus er jurist og har praktisk erfaring med databeskyttelsesret fra en stilling i Københavns Kommune. Christine er også jurist og har fra ansættelse, bl.a. som hospitalsjurist i direktionen på Amager-Hvidovre Hospital, praktisk erfaring med både databeskyttelsesretten og sundhedsretten. Med den samlede viden på persondataområdet i DPO-funktionen er der et solidt fundament for at løse opgaverne vedrørende rådgivning og overvågning på databeskyttelsesområdet, som er lovmæssigt fastlagt.

Regionen er ifølge de databeskyttelsesretlige regler forpligtet til at inddrage DPO-funktionen rettidigt og tilstrækkeligt i alle spørgsmål vedrørende beskyttelse af personoplysninger fx før offentliggørelse af udbudsmateriale eller før beslutning om sikkerhedsniveau i it-systemer.

DPO-funktionen rapporterer direkte til det øverste ledelsesniveau i regionen. DPO-funktionen er organisatorisk placeret i Center for Politik og Kommunikation, og har den daglige faglige reference til Koncerndirektionen (regionsdirektør Jens Gordon Clausen). DPO'en har holdt status- og rapporteringsmøder med direktøren ca. hver 2. måned. I 2020 lidt færre grundet Corona-situationen. DPO'en har holdt møde om funktionen samt opgaver herunder overvågning og tilsyn med regionsrådsformanden den 3. april 2019, samt orienteringsmøde med regionsrådsformanden den 6. marts 2020. Det var herefter planen at holde møder hver 2 måned, men også dette blev udsat pga. Corona-situationen.

DPO'ens aktiviteter og handlinger i løbet af perioden

DPO-funktionen har til opgave at rådgive regionen – ledelse og medarbejdere –, om deres forpligtelser i henhold til lovgivningen om databeskyttelse, overvåge efterlevelse af lovgivningen om databeskyttelse, samarbejde med Datatilsynet og være kontaktpunkt for borgerne. En opsamling af de opgaver, som DPO-funktionen har været inddraget i, er inddelt efter disse overordnede opgaver:

Rådgivning af organisationen og de ansatte om databeskyttelse

Oplæg på møder, seminarer og lignende

I den første periode var der stor fokus på at holde oplæg om databeskyttelse på møder med direktører, direktioner, sekretariater, afdelingsledelser, klinikledelser, afdelinger m.v. Møderne kom i stand både via direkte invitationer og selv-invitationer. I begyndelsen handlede det meget om at få udbredt en viden om området, så alle medarbejdere og ledere i regionen havde et - eller som minimum det samme - niveau af viden. Dvs. fokus var på relativt hurtigt at få etableret en fælles videnplatform om databeskyttelse, som DPO-funktionen og de øvrige rådgivere på området kunne bygge videre på eller tage udgangspunkt i i forbindelse med rådgivning og awareness-tiltag. Først herefter kunne den mere proaktive og værdiskabende rådgivning begynde.

Ad hoc rådgivning af ledelse og medarbejdere

Dagligt modtager DPO-funktionen henvendelser fra ledere og medarbejdere med konkrete spørgsmål eller overvejelser om, hvorvidt en given behandling af personoplysninger overholder de generelle behandlingsregler. DPO-funktionen tilstræber en proaktiv tilgang til rådgivningen. DPO-funktionen bliver ofte kontaktet af kollegaer, der ikke ved, hvor de skal gå hen for at få rådgivning på området, da der fortsat er uklarhed om, hvem der rådgiver om hvad, eller hvis de er sendt rundt i systemet uden at få den nødvendige rådgivning. I disse tilfælde guides pågældende hurtigt videre til

rette rådgivningsenhed. Som en del af DPO-funktionens proaktive tilgang inviterer funktionen ofte sig selv på møder med henblik på drøftelse af generel status på persondatasikkerheden i den konkrete afdeling eller lignende, og som ofte klarlægger områder, som bør forholdes til i forhold til de databeskyttelsesretlige regler.

Uddannelse og awareness-aktiviteter

Ambasssadør-netværk i regionen

I forbindelse med etableringen af DPO-funktionen blev der oprettet et netværk af ambassadører, hvor hver enhed i regionen udpegede en person, som skulle være bindeled mellem DPO'en og enhederne (hospitaler, centre og virksomheder). Ambassadørerne er samtidig DPO-funktionens kontaktpunkt i enhederne og en central figur i enhedernes og regionens efterlevelse af databeskyttelseslovgivningen. Sidenhen er rollen udvidet til også at være ambassadører for Videnscentret for dataanmeldelser og Sektion for Informationssikkerhed. Formålet med ambassadør-netværket er desuden at styrke kompetenceniveauet for persondataret og persondatasikkerhed i regionen. Der er pt. 19 ambassadører. Alle ambassadører deltog i en introduktionsuddannelse, første gang i august 2018, som DPO-funktionen arrangerede. Der har herefter årligt været afholdt en uddannelsesdag i 2019 og 2020. Netværket mødes en gang månedligt. DPO-funktionen står for afholdelse og planlægning af møderne. Etableringen af netværket har vist sig at fungere som planlagt. Dels er kendskabet til området højnet og dermed som et andet edderkoppespind "spredt ud over" alle enheder. Dels er der etableret et netværk ud i regionen, hvor alle ambassadører, nu hvor alle har et kontaktpunkt i alle enheder, på kryds og tværs videndeler og sparrer om konkrete problemstillinger.

Awareness og uddannelse af personalet

Al awareness-aktivitet på persondatabeskyttelsesområdet styres fra Sektion for Informationssikkerhed i Center for IT, Medico og Telefoni, dog styres nogle persondatabeskyttelsesaktiviteter på forskningsområdet af Videnscenter for dataanmeldelser i Center for Regional Udvikling (før 1. august 2020 på Rigshospitalet). Der er udarbejdet en større plan for sikkerhedskultur i regionen, som udrulles fra Sektion for Informationssikkerhed. DPO-funktionen indgår som høringspart i forbindelse med tiltag under planen for sikkerhedskultur i regionen.

Brud på persondatasikkerheden

Et brud på persondatasikkerheden skal som udgangspunkt anmeldes til Datatilsynet. I nogle tilfælde skal regionen underrette den registrerede om bruddet. I regionen er det besluttet, at det er Sektion for Informationssikkerhed, der håndterer regionens brud på persondatasikkerheden. DPO-funktionen orienteres om de konkrete brud og inddrages på initiativ fra Sektion for Informationssikkerhed i nogle tilfælde, hvor der opstår spørgsmål om den registrerede skal underrettes eller ej. Som kontaktpunkt for Datatilsynet får DPO-funktionen tilsendt alle afgørelser i anmeldte brud-sager. Som Datatilsynet selv har konstateret, i forbindelse med opgørelse af de brudsager de samlet modtager, er hovedparten af sagerne tilfælde, hvor mails er sendt til forkert modtager. Dette gælder også for

brud-sager i regionen. I regionen er der desuden en del brud-sager, hvor der er slået op på en forkert person i Sundhedsplatformen, nogle tilsigtet andre ikke tilsigtet. I forhold til brudsager, hvor mails er sendt til forkert modtager, omtaler Datatilsynet disse som "en menneskelig fejl". Dette er nok også gældende i de sager, hvor en medarbejder ved en fejl slår op på en forkert person i patientjournalen. Det er DPO-funktionens opfattelse, at disse "menneskelige fejl" fortsat er for ofte forekommende og at disse – med de rette tiltag - bør kunne minimeres yderligere.

Rådgivning i forbindelse med konsekvensanalyser

DPO-funktionen rådgiver om konsekvensanalyser, når der anmodes herom samt overvåger, at analysen opfylder de retlige regler i databeskyttelsesforordningen. Hidtil er der i regionen alene udført konsekvensanalyser for projekter omfattet af projektmodellen i Center for IT, Medico og Telefoni. Denne ledelsesbeslutning er på baggrund af DPO-funktionens anbefaling under revidering. Sektion for Informationssikkerhed står for udarbejdelse af konsekvensanalyserne. Der er udarbejdet en model for udarbejdelsen. DPO-funktionen får tilsendt konsekvensanalyserne med henblik på rådgivning, om de er korrekt gennemført, og om analysens konklusioner er i overensstemmelse med de databeskyttelsesretlige regler.

Samarbejde med Datatilsynet på vegne af organisationen

DPO-funktionen har løbende kontakt med Datatilsynet med henblik på sparring om konkrete spørgsmål i relation til regionens behandling af personoplysninger. Derudover er DPO-funktionen kontaktpunkt i forbindelse med høringer, klager fra borgere og i forbindelse med eventuelle spørgsmål til regionen vedrørende anmeldte brud på persondatasikkerheden herunder afgørelser. Ved eventuelle tilsyn orienteres DPO'en, men selve tilsynet koordineres af Sektion for Informationssikkerhed i Center for IT, Medico og Telefoni og - hvis relevant – i samarbejde med Enhed for Sundhedsforskning og Innovation i Center for Regional Udvikling. Det er DPO'ens opfattelse, at det ved et eventuelt tilsyn vil være væsentligt at sikre, at DPO'en deltager i både forberedelsen og tilsynets gennemførelse.

Kontaktpunkt for registrerede

DPO-funktionen får løbende og hyppigt henvendelser fra borgere – de registrerede -, som har spørgsmål til regionens behandling af personoplysninger eller som vil benytte de rettigheder, som følger af databeskyttelseslovgivningen. Fx retten til indsigt og sletning. Borgerne retter også henvendelse, hvis de har observeret brud på persondatasikkerheden. DPO-funktionen oplever også hyppigt, at borgere henvender sig til DPO-funktionen for at blive guidet et rigtigt sted hen i regionen. DPO-funktionen har under Corona-perioden også modtaget mange henvendelser vedrørende testtelte, coronaproever.dk, tidsbestilling generelt samt vacciner. Når borgerne også kontakter DPO-funktionen om spørgsmål, som ikke har databeskyttelsesretlig karakter, har borgerne oplyst, at det

er fordi DPO-funktionens kontaktdetaljer er de eneste konkrete kontaktinfo, som borgerne kan finde om regionen.

Samarbejdet med de øvrige enheder og afdelinger i regionen

DPO-funktionen samarbejder tæt med regionens andre rådgivningsaktører på området. Området for rådgivning om databeskyttelse i regionen er meget fragmenteret, og derfor er et tæt samarbejde en nødvendighed. DPO-funktionen rådgiver ikke om mindre praktiske eller almindelige driftsopgaver, ligesom DPO'en ikke udarbejder konkrete databehandleraftaler.

I forhold til de driftsorienterede opgaver er de centrale juridiske rådgivningsenheder Videnscentret for dataanmeldelser, som indtil den 1. august 2020 var organisatorisk forankret på Rigshospitalet og siden i Center for Regional Udvikling samt Sektion for Informationssikkerhed i Center for IT, Medico og Telefoni.

Samarbejde med de andre regioner, netværk m.v.

DPO-funktionen har et tæt samarbejde med DPO'erne i de fire andre regioner. DPO'erne mødes ca. hver anden måned og hyppigere hvis behov. DPO'erne kontakter også jævnligt hinanden ved ad hoc spørgsmål, eller hvor der er behov for sparring i forbindelse med konkrete problemstillinger – enten alle fem DPO'er eller bilateralt. DPO-funktionen har selvsagt endnu hyppigere kontakt med Region Sjælland grundet det fælles dataansvar på Sundhedsplatformen.

DPO-funktionen har et tæt samarbejde med DPO'en i Sundheds- og Ældreministeriet. DPO-funktionen deltager desuden i relevante faglige netværk med sammenlignelige organisationer i størrelse og kompleksitet i forhold til databehandlinger.

Overvågning herunder tilsyn

DPO-funktionen skal overvåge overholdelsen af databeskyttelsesforordningen, andre relevante regler på området om databeskyttelse samt interne retningslinjer for databeskyttelse. Overvågningen sker dels gennem de daglige opgaver herunder indsamling af oplysninger, der identificerer databehandlingsaktiviteter, information, rådgivning og henstillinger til ledelse og medarbejdere, dels gennem planlagte tilsyn herunder analyser og kontrol af databehandlingsaktiviteternes overholdelse af reglerne på området. Den løbende overvågning, der sker gennem konkrete opgaver, er selvsagt mere agil end planlagte tilsyn. Gennem de konkrete opgaver gives også konkrete råd, som hurtigere kan sikre, at regionen overholder lovgivningen.

Planlagte tilsyn

Der er i perioden udført 10 planlagte tilsyn. Anbefalingerne for disse tilsyn er behandlet i ledelsesgruppen KLFI – Koncernledelsens Fokusgruppe for Informationssikkerhed.

TILSYN 1	ANBEFALINGER
Regionens awareness- indsats	• DPO anbefaler, at Videnscentret for dataanmeldelser og Sektion for Informationssikkerhed udbygger det interne samarbejde vedrørende awareness- og uddannelsesaktiviteter. DPO bemærker i øvrigt, at Videnscentret og Informationssikkerhed er funktionelt og medarbejdermæssigt adskilt. Informationssikkerhed har primært i 2018 og 2019 fokuseret på det overordnede strategiarbejde på området, hvor Videnscentret havde fokus på lokale aktivitetsindsatser gennemført i form af en række relevante kurser og aktiviteter rettet mod forskere og klinikere. • Det anbefales, at awareness-aktiviteter koordineres med det arbejde, som er foregået i arbejdsgruppen for "GDPR i klinikken". • Da der allerede foreligger initiativer eller planer for awareness-tiltag, dels internt i regionen, dels eksternt på sundhedsområdet, anbefales det, at der anvendes så meget af de igangsatte eller planlagte aktiviteter som muligt, og at det vurderes om tidsplanen kan optimeres. • Det anbefales, at der i forlængelse af handlingsplanen for sikkerhedskultur udarbejdes en særskilt og samlet politik vedrørende awareness- og uddannelsesaktiviteter i forbindelse med persondatabeskyttelse, og at tiltagene tænkes ind i en strategisk fælles ramme for hele regionen med tæt inddragelse af de relevante parter i såvel klinikken som i administrationen herunder HD-kredsen og GDPR-ambassadørnetværket. • Det anbefales i den forbindelse, at ledelsen prioriterer ressourcer til awareness-dagsordenen. • Det anbefales, at awareness-tiltag sker ud fra en differentieret tilgang, og at indsatsen vurderes i forhold til den konkrete medarbejdergruppes behov eller enheds behov herunder i forhold til niveau og omfang. • Det anbefales, at der i forbindelse med ansættelse af nye medarbejdere i regionen herunder deres onboarding-forløb er fokus på awareness på persondatasikkerhed med klar styring af forløbet, og at indsatsen herunder evaluering følges tæt af ledelsen.

TILSYN 2	ANBEFALINGER
Regionens slettepolitik	• DPO anbefaler, at Region Hovedstaden understøtter Sektion for Informationssikkerheds arbejde med snarest at få udarbejdet et samlet notat (slettepolitik), der beskriver Region Hovedstadens retningslinjer eller procedurer for sletning af personoplysninger.

TILSYN 3	ANBEFALINGER
Opfølgning på Region Hovedstadens eget tilsyn med databehandlere	• DPO anbefaler, hvis dette ikke allerede er foretaget, at tilsynsmodellen justeres, så det fremgår tydeligt, at risiko- og dermed tilsynsniveau fastlægges i forbindelse med indgåelse af kontrakt/aftale. • Det anbefales, at ansvaret for systemet er klart, hvilket betyder, at der i regionen skal ske en tydelig afklaring af ansvar i forbindelse med systemforvaltning, herunder systemejerskab, systemforvalter etc.

TILSYN 4	ANBEFALINGER
GDPR-compliance (særligt fokus på kravsspecifikation) ved udbud af IT-system (HR)	• DPO anbefaler, at Center for HR og Uddannelse får indarbejdet et punkt i projektmodellen om inddragelse af DPO i forbindelse med indkøb af nye it-systemer herunder i forbindelse med udarbejdelse af kravspecifikationer til leverandører og før offentliggørelse af materialet.

TILSYN 5	ANBEFALINGER
GDPR-compliance (særligt fokus på DPIA, privacy by design, behandlingsregler) i forbindelse med indkøb af ny teknologi (robot) (Akuttelefonen)	• DPO anbefaler, at Akutberedskabet inddrager DPO for rådgivning ved overvejelser og beslutninger om, hvordan databeskyttelseslovgivningen overholdes ved regionens indkøb af nye it-systemer, kravsspecifikationer til leverandører, iværksættelse af nye behandlinger fx ved ny teknologi, indbygget databeskyttelse (privacy by design) og standardindstillinger (privacy by default). • Det anbefales, at Akutberedskabet med passende intervaller følger op på leverandøren af teknologien i forhold til GDPR-krav i både aftale og databehandleraftale. Dette gælder særligt i forbindelse med opdateringer.

TILSYN 6	ANBEFALINGER
Procedure for indrapportering af sikkerhedsbrud samt opfølgning	• På baggrund af drøftelserne vedrørende kendskab til brudproceduren i regionen, hvor Sektion for Informationssikkerhed påpegede en udfordring i forhold til sene indberetninger, anbefaler DPO at det overvejes, om der bør iværksættes ekstra og supplerende tiltag - udover gennem program for sikkerhedskultur – i forhold til at udbrede kendskabet til proceduren, så indberetning af brud sker hurtigere med henblik på hurtigere intern håndtering i Informationssikkerhed og afrapportering til Datatilsynet. • Det anbefales endvidere at indsætte dokumentation for de juridiske vurderinger af indberetninger i regionens dokumentationslog herunder begrundelsen for vurderingerne.

TILSYN 7	ANBEFALINGER
Fysiske sikkerhedskrav til persondatabeskyttelse	• DPO anbefaler, at regionen har fokus på at sikre, at følsomme oplysninger ikke ligger frit tilgængeligt på hospitalernes arbejdsområder, så uvedkommende har adgang til oplysningerne, og at der i den forbindelse ses på, hvordan der kan ske aflåsning eller tilsvarende i forbindelse med tilgang til følsomme oplysninger i fysisk form på hospitalernes arbejdsområder fx enten via lås på døre, tydelig afmærkning eller containere. Regionen bør undersøge, om man kan lette adgangsforholdene for medarbejderne via en teknisk enkel løsning som fx adgangskort med chip. • DPO anbefaler, at regionen udarbejder en procedure for, hvordan regionens chauffører foretager kontrol af de sikrede affaldscontaineres placering, når chaufførerne udfører sædvanlige arbejdsopgaver i forbindelse med afhentning, håndtering og transport. En procedure bør også forholde sig til den elektroniske tidsmæssige logning, som allerede foregår, herunder eventuelle persondataretlige spørgsmål. DPO bør inddrages i relevant omfang. • DPO anbefaler, at der som en del af regionens proces med indførelse af fysiske sikkerhedsprocedurer vedrørende personoplysninger på hospitalerne etableres en tilsynsordning, der fx kan håndteres af Sektion for Informationssikkerhed.

TILSYN 8	ANBEFALINGER
Implementering af proces for udarbejdelse af DPIA i Region Hovedstaden	• DPO anbefaler, at der holdes et opfølgende møde mellem Sektion for Portefølje og DPO med henblik på optimering af den implementerede proces. • Det anbefales, at ledelsesbeslutning om, at analysen om udarbejdelse af DPIA kun sker for projekter omfattet af Center for IT, Medico og Telefoni's projektmodel, revurderes og udvides til også at omfatte andre projekter og databehandlinger i regionen.

TILSYN 9	ANBEFALINGER
Indgåelse af databehandleraftaler med databehandlere	• DPO anbefaler, at der skabes større klarhed over, hvor regionens databehandleraftaler opbevares, herunder hvem der har ansvaret for at udarbejde aftalerne. • DPO anbefaler, at der etableres en tydelig proces i forhold til aktindsigtsanmodninger vedrørende databehandleraftaler, så der er klarhed over, hvilke parter der skal involveres, herunder hvor de pågældende databehandleraftaler kan fremfindes herunder i hvilke enheder.

TILSYN 10	ANBEFALINGER
Proces for tildeling af VPN-adgang til eksterne leverandører til regionens driftsmiljø	• DPO anbefaler, at blanketter og retningslinjer opdateres, så de er tidssvarende. • Det anbefales, at processer for administration, herunder tildeling og lukning af VPN-adgange dokumenteres, og der fastlægges en klar ansvarsfordeling.

Opsamling og fremtidige aktiviteter

Region Hovedstaden har arbejdet intenst med databeskyttelsesområdet både før og efter databeskyttelsesforordningen trådte i kraft i 2018. Arbejdet er gået fra projekt til drift, og er kommet meget langt siden maj 2018 med gode resultater. Processen har betydet en betydelig modning for regionen i takt med, at der er iværksat nye tiltag. Det betyder også, at regionen i dag er på et andet niveau end i maj 2018 både med hensyn til indsatser som krav til både medarbejdere og ledelse. DPO-funktionen oplever i dag generelt et passende bevidsthedsniveau alle steder i regionen, og derfor kan der i dag stilles lidt højere krav til den daglige håndtering af personoplysninger og sundhedsdata herunder også i forhold til juridisk compliance.

Der er udarbejdet et omfangsrigt rammeværk for behandling af personoplysninger, sundhedsoplysninger og it-sikkerhed, som har givet en struktur på informationssikkerhedsområdet, og det er godt. Samtidig er det – netop set i lyset af det højere modenhedsniveau - vigtigt at fastholde fokus på, at struktur alene ikke skaber den gode og tilstrækkelige databeskyttelse i forbindelse med håndtering af regionens person- og sundhedsoplysninger. Vejledninger og it-systemer med "privacy by design" hjælper os kun noget af vejen. En kombination af 45.000 personer med jævnlig udskiftning på pladserne, ny teknologi og en hektisk hverdag betyder alt andet lige, at der løbende vil være et behov for at holde fokus på, hvordan vi håndterer data i regionen: Det gælder både i de komplekse sager, som fx udvikling og anvendelse af AI og i forbindelse med de mange tusinder af mails, der hver dag sendes i og fra regionen. I alle tilfælde er der mennesker involveret. Dette betyder også, at regionen er særligt eksponeret for "den menneskelige fejl", som kan have lige så katastrofale konsekvenser for datasikkerheden, som en teknisk fejl. Derfor ligger der også fortsat en vigtig opgave for ledelsen i at erindre medarbejderne om den korrekte databehandling, som gælder lokalt. Vi er så at sige ikke stærkere end det svageste led. Der er igangsat et godt regionalt program for awareness på området, men dette gør det ikke alene og bør bl.a. løbende suppleres af lokal italesættelse og fokus - naturligvis tilpasset de lokale forhold.

Selvom persondataretlig compliance er en kontinuerlig opgave, er det DPO-funktionens opfattelse, at Region Hovedstaden alt i alt er godt på vej. Dette gælder også, når vi sammenligner os med andre myndigheder og virksomheder. Vi ser ind i et 2021, hvor regionen efter DPO-funktionens opfattelse vil tage et ekstra ryk fremad i forhold til modenhed på databeskyttelsesområdet, men hvor vi også udfordres af ny teknologi, nye muligheder og højere compliancekrav. Vi ser derfor også ind i et 2021, hvor der bør stilles større krav til compliance-håndtering i de lokale processer. DPO-funktionen vil derfor opfordre til, at der fortsat er fokus på digitalisering, og at der hyppigere sker politiske drøftelser af "teknologi og sundhedsområdet" i forhold til muligheder, visioner og strategi. Baseret på den erfaring, vi har gjort os i forhold regionens indsats på området samt de fokusområder, som Datatilsynet har lanceret som tilsynsområder, finder DPO-funktionen det relevant i 2021 at foretage overvågning af bl.a. biobanker, tilsyn med databehandlere på forskningsområdet, AI-området særligt i forhold til håndtering af compliancekrav og struktureret tilgang samt en transparent og sammenhængende juridisk rådgivning på forskningsområdet, der sikrer compliance.

DPO-funktionen ser frem til at fortsætte det gode samarbejde med rådgivningsfunktionerne i regionen og regionens ledelse og medarbejdere.

Region Hovedstaden

Region Hovedstaden
Center for Politik og Kommunikation

DPO-funktionen

Kongens Vænge 2
3400 Hillerød