Region Hovedstaden

**Center for Politik og Kommunikation**

Ledelsesbetjening og -kommunikation

**NOTAT**

Til: Forretningsudvalget i Region Hovedstaden

Dato: 25. maj 2021

# Administrationens opfølgning på DPO-rapport for 2020

Regionsrådet tog på sit ordinære møde den 20. april 2021 databeskyttelsesrådgiverens rapportering for 2020 til efterretning og anmodede om, at DPO'en deltager på et kommende forretningsudvalgsmøde (den 11. maj) med henblik på at uddybe rapporten, og hvor ledelsen samtidig kan orientere nærmere om opfølgningen fremadrettet.

Rapporten beskriver DPO'ens funktion og arbejdsopgaver, herunder en opsamling på overvågningsdelen, inklusiv anbefalinger og rådgivning, som er givet i forbindelse med ti planlagte tilsyn, udført i 2019 og efterbehandlet i 2020.

Regionen redegør i dette notat for den lokale opfølgning på DPO-rapportens anbefalinger, der vedlægges som bilag til FU-sagen.

| Anbefaling fra DPO | Svar fra administrationen |
|---|---|
| **1. Regionens awarenessindsats** | |
| 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.<br><br>Det anbefales, at awarenessaktiviteter koordineres med det arbejde, som er foregået i arbejdsgruppen for "GDPR i klinikken".<br><br>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.<br><br>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.<br><br>Det anbefales i den forbindelse, at ledelsen prioriterer ressourcer til awareness-dagsordenen.<br><br>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.<br><br>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. | Sektion for Informationssikkerhed og Videnscenter for Dataanmeldelser er løbende i dialog om aktiviteter på informationssikkerheds- og databeskyttelsesområdet, ligesom regionens GDPR-netværk inddrages løbende i forhold til awareness-aktiviteterne i regionen.<br><br>Koncernledelsen godkendte i juni 2019 et samlet program for sikkerhedskultur, som herefter udgør den strategiske ramme og plan for regionens uddannelses- og kommunikationsindsatser vedr. informationssikkerhed og databeskyttelse. Prioritering af regionens awareness-tiltag foretages ud fra denne ramme.<br><br>Programmets første fase har primært haft fokus på at sikre, at alle medarbejderne har den fornødne grundlæggende viden og kompetencer på plads. Behovet for specialiserede indsatser til særlige målgrupper vil indgå i planlægningen af kommende faser i programmet.<br><br>Onboarding-forløb med e-læring er en del af program for sikkerhedskultur, som blev gennemført i 2020 i samarbejde med Center for HR og Uddannelse. I den forbindelse blev de regionale jobstartssider, kodebrevsmail og ansættelsesbrev til nye medarbejdere og brugere opdateret, og der lanceredes et nyt obligatorisk e-læringskursus for nye medarbejdere i regionen. Herudover modtager alle nye medarbejdere fortsat folderen "Beskyt vores data" digitalt som pdf. sammen med deres ansættelsesbrev.<br><br>Der rapporteres fra 2021 løbende på gennemførsel af e-læringskursus for alle medarbejdere i regionen som led i den generelle ledelsesrapportering om informationssikkerhed og databeskyttelse. Herudover modtager hospitaler, virksomheder og koncerncentre kvartalsvis i hele 2021 status på udrulning af e-læringskurset til både nye og eksisterende medarbejdere.<br><br>Tidsplan og prioriteringer ift. awarenessaktiviteter følges løbende af Koncernledelsens Fokusgruppe for Informationssikkerhed. |

**2. 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. | På baggrund af DPO'ens anbefaling om en samlet slettepolitik for regionen indarbejdedes rammerne for sletning i regionens retningslinjer for databeskyttelse, særligt i form af en supplerende retningslinje for opbevaring og sletning. Retningslinjen godkendtes af Koncernledelsens Fokusgruppe for Informationssikkerhed d. 9. oktober 2020. |

**3. 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.<br><br>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. | Sektion for Informationssikkerhed tager anbefalingerne vedr. fastlæggelse af tilsynsniveau ved kontraktindgåelse, samt fastlæggelse af ansvar for den indkøbte løsning til efterretning. Regionen har samlet vurderet, at der ikke iværksættes særskilte opfølgningsaktiviteter efter faglig vurdering af Sektion for Informationssikkerhed og efterfølgende drøftelse i Koncernledelsens Fokusgruppe for Informationssikkerhed. Denne vurdering er foretaget en ud fra en samlet afvejning af bl.a. DPO-anbefalingen og hensynene til allerede igangværende og kommende aktiviteter i regionen på området. |

**4. 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. | Tilsynsrapporten og anbefalingen er gennemgået med de relevante enheder i Center for HR og Uddannelse med henblik på at sikre forankring og opfølgning. Der er i forbindelse med projektmodellen for indkøb af nye systemer tilføjet en anbefaling 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.<br><br>Center for HR og Uddannelse har udarbejdet en fast proces for opfølgning, som indebærer systematisk gennemgang af revisionsrapporter og årlig opfølgning på eventuelle bemærkninger i revisionserklæringer årligt herunder ift. leverandørerne.<br><br>I forhold til leverandørerne efterspørges en handlingsplan for opfølgningspunkter med fokus på adgang til personoplysninger og sikkerhed. Anmærkninger vurderes efter kritikalitet og der sker en årlig opfølgning på, om bemærkningspunkter kan lukkes. På et mere overordnet plan følger Center for HR og Uddannelse løbende Datatilsynets praksis blandt andet med henblik på løbende at opdatere kravsspecifikationer i henhold til eventuel ny praksis. |

**5. GDPR-compliance i forbindelse med indkøb af ny teknologi (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).<br><br>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. | Medio 2019 havde Akutberedskabet DPO-tilsyn vedr. indkøb af teknologi i form af AI (kunstig intelligens). AI er et Corti-produkt, der har til formål at hjælpe det sundhedsfaglige personale ved 1-1-2 med hurtig erkendelse af hjertestop hos borgere. Projektet er et forskningsprojekt – der er ikke tale om anskaffelse af robotteknologi med dertilhørende udbudsmateriale. Corti er databehandler på projektet og bistår med maskinel transskribering og mønstergenkendelse i samtaler med 1-1-2 på Regionens Vagtcentral. Corti leverer software, som analyserer samtalerne. Analyserne foregår på et computersystem inden for regionens netværk, som er placeret i Akutberedskabets serverrum.<br><br>Projektet er godkendt af Sektion for Informationssikkerhed den 6. februar 2018. Godkendelsen er sket på baggrund af et udarbejdet anmeldelsesskema, sikkerhedsskema samt databehandleraftale med Corti. Projektet er påbegyndt før, de nye databeskyttelsesregler trådte i kraft, hvorfor Akutberedskabet anser godkendelsen som dækkende i forhold til spørgsmålet om konsekvensanalyse (DPIA). Akutberedskabet samarbejder med Center for IT, Medico og Teknologi om at implementere it-infrastruktur til maskinlæring i regionens eksisterende server-park. Endvidere skal der etableres en fiber-forbindelse til Computerome, og herunder skal der i regi af Center for IT, Medico og Telefoni udarbejdes et System-Etablerings-Dokument. Akutberedskabet vil udarbejde en konsekvensanalyse (DPIA), og indbygget databeskyttelse (”privacy by design”) vil blive indtænkt. DPO vil ligeledes blive inddraget efter konkret vurdering og behov. |

**6. Procedure for indberetning 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.<br><br>Det anbefales endvidere at indsætte dokumentation for de juridiske vurderinger af indberetninger i regionens dokumentationslog herunder begrundelsen for vurderingerne. | Regionen har samlet vurderet efter faglig indstilling af Sektion for Informationssikkerhed og efterfølgende drøftelse i Koncernledelsens Fokusgruppe for Informationssikkerhed, at håndteringen af persondatabrud er fortsat efter den fastsatte procedure. Der er i forvejen planlagt information om brudproceduren i de produkter, der er planlagt i regionens program for sikkerhedskultur. Anbefalingen vedr. dokumentation af den juridiske vurdering er implementeret, og der igangsættes ikke yderligere opfølgningsaktiviteter. Denne vurdering er foretaget en ud fra en samlet afvejning af bl.a. DPO-anbefalingen og hensynene til allerede igangværende og kommende aktiviteter i regionen på området.<br><br>Proceduren for brud på persondatasikkerheden er som led i den løbende opfølgning på området justeret og godkendt af Koncernledelsens Fokusgruppe for Informationssikkerhed i marts 2021. |

## 7. Fysiske krav 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.<br><br>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.<br><br>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. | Center for Ejendomme (CEJ) har udarbejdet procedurer for hospitalerne, der beskriver ansvar, herunder CEJ´s ansvar for den del af processen der vedrører sikker bortskaffelse, når papir og plasticaffald er smidt i anvendte containere og frem til destruktion. Regionens hospitaler er selv ansvarlige for at udarbejde lokale sikkerhedsprocedurer i forbindelse med bortskaffelse af papir- og plasticemballage med personfølsomme oplysninger på hospitalerne.<br><br>Regionen gennemfører kontrolprocedurer af de sikrede affaldscontaineres placering i forbindelse med afhentning/håndtering/transport, har etableret elektronisk tidsmæssig logning og har efterfølgende udskiftet affaldscontainerne til papir med aflåselige containere samt aflåste makuleringsspande. Center for Ejendomme er i løbende dialog med de fire hospitaler (Gentofte, Bornholm, Bispebjerg og Hvidovre), der pt. har indført eller er i færd med at indføre fysiske sikkerhedsprocedurer. For resterende hospitaler vil en lignende dialog starte op.<br><br>Center for Ejendomme arbejder på pilotprojektet ”Èt fælles ID kort”, der har fokus på:<br><br>• At sikre lettere adgangsforhold for medarbejdere via en teknisk enkel løsning som fx adgangskort med chip<br>• At sikre, at følsomme oplysninger ikke ligger frit tilgængeligt på hospitalernes arbejdsområder,<br>• At sikre 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. |

## 8. Implementering af proces for udarbejdelse af DPIA i Region Hovedstaden

| | |
|---|---|
| DPO anbefaler, at der holdes et opfølgende møde mellem Sektion for Porteføljе og DPO med henblik på optimering af den implementerede proces.<br><br>Det anbefales, at ledelsesbeslutning om, at analysen om udarbejdelse af DPIA kun sker for projekter omfattet af Center for IT, Medico og Telefonis projektmodel, revurderes og udvides til også at omfatte andre projekter og databehandlinger i regionen. | Tilsynet omhandler regionens proces for udarbejdelse af konsekvensanalyser i forbindelse med indkøb af visse IT-systemer i Region Hovedstaden. En konsekvensanalyse hedder på engelsk en ”data privacy impact assesment” og forkortes DPIA. En konsekvensanalyse indeholder typisk en afvejning af de ønskede behandlinger af personoplysninger, om behandlingerne er nødvendige og afmålte i forhold til det man vil opnå, og hvordan man vil håndtere de risici, der opstår ved persondatabehandlingerne. |

| | |
|---|---|
| | I forhold til andet tilsynspunkt besluttede Koncernledelsens Fokusgruppe for Informationssikkerhed d. 9. oktober, at processens omfang udvides bredt i en periode på seks måneder, hvor alle hospitaler, virksomheder og centre får mulighed for at melde aktiviteter ind til DPIA-screening i Sektion for Informationssikkerhed. Som opfølgning på denne seksmåneders-periode skal Sektion for Informationssikkerhed evaluere og forelægge regionens erfaringer for samt komme med konkrete anbefalinger til det fremadrettede procesomfang til Koncernledelsens Fokusgruppe for Informationssikkerhed. |

**9. 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.<br><br>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. | Der pågår aktuelt dialog mellem Center for IT, Medico og Telefoni og Center for Regional Udvikling i forhold til at justere på opgavefordelingen mellem de centrale juridiske rådgivningsfunktioner (hhv. Videnscenter for Dataanmeldelser og Sektion for Informationssikkerhed), således at ansvarsfordelingen bliver mere tydelig og lettere for organisationen at navigere i.<br><br>Regionen vil som opfølgning på DPO-anbefalingen om aktindsigtsanmodninger vedrørende databehandleraftaler foretage en opfølgende vurdering af regionens proces på området. Anbefalingen medtages også i den løbende udvikling af regionens procedure og rammer for håndtering af databehandleraftaler. |

**10. Proces for tildeling af VPN-adgange til eksterne leverandører til regionens driftsmiljø**

| | |
|---|---|
| DPO anbefaler, at blanketter og retningslinjer opdateres, så de er tidssvarende.<br><br>Det anbefales, at processer for administration, herunder tildeling og lukning af VPN-adgange dokumenteres, og der fastlægges en klar ansvarsfordeling. | Bestilling og efterfølgende tildeling af VPN til eksterne leverandører foregår gennem regionens change-proces, hvor der i processen er indeholdt relevante godkendelser og en fast ansvarsfordeling.<br><br>Tildeling af en VPN adgang er en ”standard-change”, hvor dokumentationen følger de almindelige standarder for dokumentation i change-processen, herunder bl.a. udfyldt blanket fra den eksterne leverandører.<br><br>Blanketten indeholder oplysninger om de pågældende brugere, der skal have adgang og den opdateres efter behov. |