Databeskyttelsesrådgiverens årsrapport 2018

www.rsyd.dk

Region Syddanmark

Indhold

Indledning

25. maj 2018 var et historisk øjeblik i databeskyttelsesretten. Fra denne dag skulle nye EU-regler for behandling af personoplysninger nemlig anvendes. Reglerne kaldes i daglig tale databeskyttelsesforordningen eller GDPR.

De nye EU-regler beskytter de mennesker, hvis oplysninger bliver behandlet. Reglerne skal sikre borgernes ret til privatliv og skabe tillid til myndigheders håndtering af borgernes oplysninger.

Disse regler er således også gældende for Region Syddanmark. I regionens varetagelse af sine kerneopgaver, særligt på sundhedsområdet, behandles store mængder personoplysninger. I løsningen af regionens opgaver skal der derfor også tages højde for kravene i databeskyttelsesretten.

Denne årsrapport er den første af sin slags fra Region Syddanmarks databeskyttelsesrådgiver.

Formålet med den er at oplyse om databeskyttelsesrådgiverens arbejde i 2018 samt give konkrete anbefalinger for regionens arbejde med databeskyttelsen i 2019.

Mia Bekker Leimand

Databeskyttelsesrådgiver, Region Syddanmark
17. januar 2019

Præsentation af databeskyttelsesforordningen og databeskyttelsesrådgiveren

Kort om databeskyttelsesforordningen

Databeskyttelsesforordningen eller GDPR[1] regulerer, hvornår og hvordan dataansvarlige må behandle personoplysninger. Databeskyttelsesforordningen suppleres i Danmark af databeskyttelsesloven.

Forordningen og loven er relevante for Region Syddanmark, hver gang regionen indsamler, opbevarer og videregiver personoplysninger om borgere, ansatte og patienter. Region Syddanmark er den såkaldte "dataansvarlige".

Databeskyttelsesforordningen stiller en række krav, der skal opfyldes, når regionen behandler personoplysninger. Kravene minder i høj grad om dem, der fremgik af den tidligere gældende persondatalov.

Det nye er især, at dataansvarlige skal kunne dokumentere, at reglerne bliver efterlevet. Hvor regionen førhen skulle anmelde behandling af personoplysninger til Datatilsynet, er det nu regionens opgave at have et overblik i en intern fortegnelse over behandlingerne.

Hertil kommer, at regionen skal iværksætte passende sikkerhed på baggrund af en risikovurdering f.eks. i IT-systemer. Endvidere skal regionen anmelde brud på persondatasikkerheden til Datatilsynet.

Udpegelse af databeskyttelsesrådgiver

Det er også et nyt krav, at offentlige myndigheder skal udpege en databeskyttelsesrådgiver (DPO[2]).

1. marts 2018 tiltrådte databeskyttelsesrådgiveren som databeskyttelsesrådgiver i Region Syddanmark.

DATABESKYTTELSESFORORDNINGEN

- **Erstatter EU-direktiv 95/46 og persondataloven samt sikkerhedsbekendtgørelsen.**
- **Kaldes ofte GDPR.**
- **Skulle anvendes i dansk ret fra 25. maj 2018.**
- **Suppleres af den nye databeskyttelseslov.**
- **Retten til databeskyttelse findes i EU's charter om grundlæggende rettigheder.**
- **Retten til privatliv er beskyttet i FN's verdenserklæring såvel som EU's charter samt den europæiske menneskerettighedskonvention.**

1) GDPR = General Data Protection Regulation (Forordning 2016/679 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF).

2) DPO = Data Protection Officer er den engelske betegnelse for databeskyttelsesrådgiver.

Databeskyttelsesrådgiverens stilling

Regionen er forpligtet til at inddrage databeskyttelsesrådgiveren tilstrækkeligt og rettidigt i alle spørgsmål vedrørende behandling af personoplysninger f.eks. før offentliggørelse af udbudsmateriale eller før beslutning om sikkerhedsniveau i IT-systemer.

Regionen er også forpligtet til at støtte databeskyttelsesrådgiveren i udførelsen af sine opgaver, bl.a. ved at tilvejebringe ressourcer og give adgang til personoplysninger og behandlingsaktiviteter.

Databeskyttelsesrådgiveren må ikke modtage instrukser om udførelsen af sine opgaver; der skal være uafhængighed. Databeskyttelsesrådgiveren må ikke straffes eller sanktioneres for at udføre opgaverne. Databeskyttelsesrådgiveren er i sine ansættelsesvilkår beskyttet af de særlige regler om afskedigelse og andre væsentlige stillingsændringer, som er gældende for tillidshverv, ligesom tillidsrepræsentanter.

Databeskyttelsesrådgiveren skal rapportere direkte til det øverste ledelsesniveau hos den dataansvarlige.

Databeskyttelsesrådgiveren i Region Syddanmark er organisatorisk placeret i Råds- og direktionssekretariatet, og har faglig reference til regionsdirektøren.

Databeskyttelsesrådgiverens opgaver

Forordningen fastsætter i vidt omfang databeskyttelsesrådgiverens opgaver. Det fremgår, at databeskyttelsesrådgiveren skal:

- varetage sine opgaver under hensyn til de risici, der er forbundet med behandlingen af personoplysningerne.
- rådgive og være med til at sikre, at regionen overholder forpligtelserne i databeskyttelsesforordningen. Denne opgave omfatter blandt andet undervisning til regionens ansatte.
- kontrollere, at kravene efterleves. Dette gælder både kravene, der følger af forordningen og krav, der følger af anden lovgivning samt kravene, som regionen fastsætter i retningslinjer om beskyttelse af personoplysninger fx vedrørende fordeling af ansvar, oplysningskampagner og uddannelse af regionens ansatte.
- hjælpe med at udarbejde konsekvensanalyser, som er databeskyttelsesretlige risikovurderinger, hvor risiciene for de registreredes ret til databeskyttelse analyseres og mindskes.
- fungere som kontaktpunkt for registrerede og Datatilsynet.

Endelig skal databeskyttelsesrådgiveren sørge for årlig rapportering til regionsrådet i form af denne rapport.

Resultater for 2018

Introduktion og opstart

Databeskyttelsesrådgiveren skal være tilgængelig for de registrerede (borgere og medarbejdere).

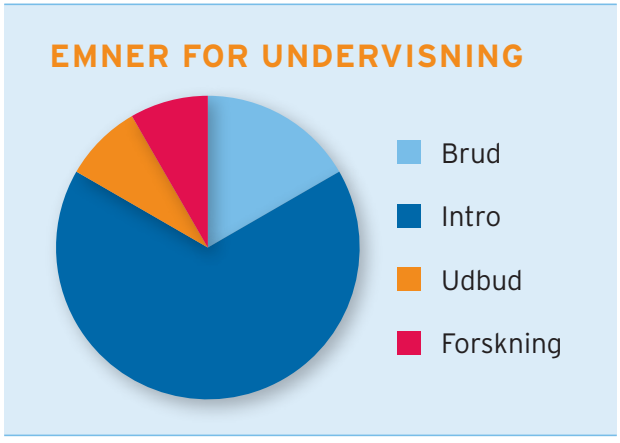
Derfor var én af de første opgaver at udarbejde en side på regionens hjemmeside: **www.regionsyddanmark.dk/dpo**, hvor borgeren kan læse om databeskyttelsesrådgiveren, dennes opgaver og finde kontaktoplysninger.

Databeskyttelsesrådgiveren har fået en sikker postkasse, som borgere kan skrive til. Derudover kan borgeren skrive til databeskyttelsesrådgiveren direkte fra deres e-Boks.

I april 2018 blev databeskyttelsesrådgiveren præsenteret på regionens fællesregionale intranet med interview og billede samt kontaktoplysninger, så regionens medarbejdere kan finde frem til databeskyttelsesrådgiveren. Endvidere er databeskyttelsesrådgiveren blevet introduceret på en morgenbriefing for regionshusets ansatte.

Funktionsbeskrivelse og afklaring af snitflader

I introduktionsfasen påbegyndte databeskyttelsesrådgiveren en afklaring af snitflader til andre afdelinger i regionen. Særligt i forhold til Afdeling for Informationssikkerhed er der aftalt fordeling af arbejdsopgaver med fagligt overlap.



Denne fordeling er dokumenteret i databeskyttelsesrådgiverens funktionsbeskrivelse.

Funktionsbeskrivelsen redegør for databeskyttelsesforordningens krav til databeskyttelsesrådgiveren, lige som den indeholder en procedure for det tilfælde, at databeskyttelsesrådgiverens rådgivning ikke bliver fulgt.

Funktionsbeskrivelsen oplister de ressourcer (IT-udstyr, programmer og uddannelsesforløb), som databeskyttelsesrådgiveren har til rådighed. Databeskyttelsesrådgiveren indgår som en del af Råds- og direktionssekretariatet og har ikke eget budget.

Undervisning ("awareness")

Et vigtigt element i regionens overholdelse af kravene er bevidsthed om, hvorfor og hvornår kravene skal opfyldes, men også egentlig uddannelse i, hvad der kræves af den enkelte medarbejder.

Der er udarbejdet informationsmateriale i form af film, plakater og artikler, som kan tilgås via temasider på intranettet, **intra.reg.rsyd.dk/it/informationssikkerhed/Sider/default.aspx**

Databeskyttelsesrådgiveren har undervist flere end 300 kolleger i 2018. Størstedelen af deltagerne har efterspurgt en generel introduktion til kravene, men der er også undervist specifikt i brud på persondatasikkerheden, personoplysninger i udbudsretten og særreglerne inden for forskning.

Der er fortsat høj efterspørgsel på information og materiale.

Retningslinjer

Med udgangspunkt i IT-sikkerhedsstandarden ISO 27001 er der udarbejdet og godkendt en række nye retningslinjer inden for informationssikkerhed.

Retningslinjerne er godkendt i Udvalg for Informationssikkerhed (UFI), hvor databeskyttelsesrådgiveren også deltager.

Indsigtsanmodninger – retten til indsigt

Retten til indsigt er en rettighed, der følger af databeskyttelsesforordningen, og som minder om retten til aktindsigt. Retten til indsigt adskiller sig typisk ved, at den kan omfatte alle regionens behandlinger om en registreret (borger, patient, medarbejder m.v.) dvs. alle personoplysninger, som Region Syddanmark har om en person, på tværs af regionen.

I 2018 har databeskyttelsesrådgiveren sammen med en række interessenter fra regionshuset og sygehusene udarbejdet en retningslinje for behandling af indsigtsanmodninger, så de tværgående indsigtsanmodninger kan håndteres korrekt og rettidigt.

Brud på persondatasikkerheden

Et brud på persondatasikkerheden er et brud på personoplysningernes fortrolighed, integritet eller tilgængelighed. Et brud kan ses som en slags utilsigtet hændelse for personoplysninger, og ligesom de utilsigtede hændelser skal bruddene bruges til at lære og til at kvalitetssikre persondatasikkerheden. Brud skal anmeldes til Datatilsynet. I nogle tilfælde skal regionen underrette de berørte personer om bruddet, så de kan træffe egne forholdsregler.

Datatilsynet sender efter anmeldelsen typisk en række spørgsmål, som regionens systemejer besvarer i samarbejde med databeskyttelsesrådgiveren eller Afdeling for Informationssikkerhed. På baggrund af disse oplysninger kan Datatilsynet vælge at henlægge sagen og ikke foretage sig yderligere, at give et påbud eller anden administrativ sanktion eller at politianmelde regionen for overtrædelse af databeskyttelsesreglerne.

Ethvert brud anmeldes i første omgang til Afdeling for Informationssikkerhed, som fører en liste over antal brud, type, årsag, system, ansvarlig enhed m.v.

BRUD - EKSEMPLER

- Medarbejdere har adgang til oplysninger, de ikke bør have adgang til
- Medarbejder ændrer eller sletter personoplysninger ved et uheld
- Utilsigtet videregivelse f.eks. mail til forkert modtager
- Manglende kryptering af hjemmeside
- Ikke tilgængeligt IT-system pga. hackerangreb

Ultimo december 2018 er status:

- Total: 25 anmeldte brud til Datatilsynet.
- 16 brud skyldtes utilsigtet videregivelse af personoplysninger.
- 8 skyldtes utilsigtet adgang til personoplysninger i regionens systemer
- 1 årsag er ikke endeligt fastslået endnu

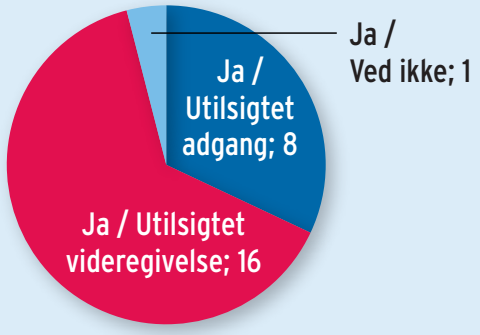
10 af 25 brud er sket fra Outlook – typisk fordi medarbejdere kommer til at sende en mail til den forkerte modtager.

Langt de fleste brud er opgjort som menneskelige fejl i modsætning til hhv. systemfejl og deciderede ondsindede handlinger f.eks. hackerangreb.

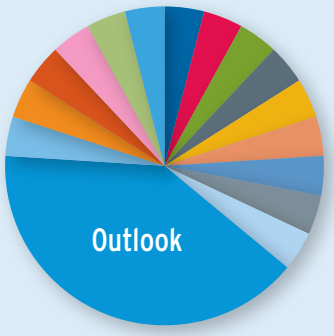
Kun et fåtal af regionens anmeldte brud er indtil videre afgjort af Datatilsynet, og heraf har Datatilsynet henlagt de fleste uden sanktioner.

Region Syddanmark har dog modtaget kritik for et brud på persondatasikkerheden i et system, som efter tilsynets vurdering ikke levede op til det påkrævede sikkerhedsniveau. Det skyldtes, at personoplysninger om et stort antal patienter potentielt kunne tilgås af alle regionens ansatte i en lang periode, og at det – med en vis lægefaglig viden – var muligt at udlede helbredsoplysninger.

ANMELDTE BRUD TOTAL



BRUD SKET FRA OUTLOOK



STATUS ULTIMO DECEMBER 2018

Tilsyn

Datatilsynet har af egen drift henvendt sig til Region Syddanmark i forbindelse med et tilsyn om, hvorvidt regionen havde udpeget en databeskyttelsesrådgiver herunder for selve regionen og dennes underlæggende myndigheder og organer, der f.eks. tæller hospicerne. På tidspunktet for Datatilsynets henvendelse, var databeskyttelsesrådgiveren udpeget som databeskyttelsesrådgiver for regionen, men kun få underlæggende myndigheder og organer havde udpeget en databeskyttelsesrådgiver.

Som resultat af tilsynet blev databeskyttelsesrådgiveren udpeget som databeskyttelsesrådgiver for de resterende underlæggende myndigheder og organer til regionen.

Audit

Databeskyttelsesrådgiveren skal kontrollere, at Region Syddanmark overholder databeskyttelsesforordningens krav til behandling af personoplysninger. Derfor blev der i 2018, i samarbejde med Afdeling for Informationssikkerhed, foretaget audit af aftalegrundlaget for IT-systemerne COSMIC, Cetrea og BCC.

Auditten er den første interne audit vedrørende informationssikkerhed, og den skulle derfor også bruges som træning. Som led i auditten blev databehandleraftalerne mellem regionen og dennes leverandører gennemgået. Audittens resultater er beskrevet i en auditrapport, som er forelagt Udvalg for Informationssikkerhed (UFI).

Procedure ved uenighed

I det tilfælde, at databeskyttelsesrådgiverens rådgivning ikke bliver fulgt, er det i databeskyttelsesrådgiverens funktionsbeskrivelse beskrevet, at regionsrådet skal orienteres om det i årsrapporten.

Indebærer et brud på persondatasikkerheden en risiko for de registrerede, skal bruddet anmeldes til Datatilsynet. Hvis et brud på persondatasikkerheden indebærer en **høj** risiko for de registrerede, har det betydning for, hvorvidt regionen er forpligtet til at orientere de berørte personer herom, herunder hvorvidt der skal orienteres via en pressemeddelelse. Sidstnævnte kan regionen være forpligtet til, hvis det ikke kan lade sig gøre at orientere individuelt.

I 2018 har der i to konkrete tilfælde være forskellige opfattelser af begrebet "høj risiko for de registrerede". I 2019 opdateres regionens retningslinje for håndtering af brud på persondatasikkerheden, hvorefter vurderingen af, om der er **høj** risiko forbundet med bruddet foreslås foretaget af Afdeling for Informationssikkerhed. Afdelingen foretager allerede i dag vurderingen af, hvorvidt der er en risiko forbundet med bruddet.

Anbefalinger for 2019

På baggrund af databeskyttelsesrådgiverens aktiviteter og resultater for 2018 gives følgende konkrete anbefalinger til regionens arbejde i 2019.

ANBEFALINGER FOR 2019

Iværksættelse af yderligere awareness-tiltag

Det er databeskyttelsesrådgiverens indtryk, at regionens medarbejdere efterspørger uddannelse i de databeskyttelsesretlige krav. Hertil kommer, at de fleste brud på persondatasikkerheden skyldes menneskelige fejl. På den baggrund anbefales det at etablere et e-learningsmodul eller tilsvarende, der kan skabe øget awareness omkring reglerne for behandling af personoplysninger.

Styrkelse af introduktionen af ny IT

Niveauet af sikkerhed i IT-systemer skal fastsættes på baggrund af en risikovurdering. Her tages der højde for, hvilken risiko for borgerens privatliv, der er forbundet med behandlingen af personoplysninger. Databeskyttelsesrådgiveren anbefaler, at der fortsat foretages risikovurderinger på IT-systemer, og at det sikres, at nye IT-systemer også risikovurderes, inden de implementeres.

Udarbejdelse af konsekvensanalyser

Databeskyttelsesrådgiveren anbefaler, at der udarbejdes konsekvensanalyser for:

- EPJ SYD
- Region Syddanmarks sikkerhedsforanstaltninger, der overvåger eller kontrollerer regionens medarbejdere (f.eks. intrution detection system og logning)
- Business Intelligence-systemet

En konsekvensanalyse er en databeskyttelsesretlig risikovurdering, hvor risiciene for de registreredes ret til databeskyttelse analyseres og mindskes.

Styrkelse af adgangskontrol

Omtrendt halvdelen af regionens brud på persondatasikkerheden i 2018 er forårsaget af utilsigtet adgange til personoplysninger. Det skal sikres, at regionens medarbejdere kun har adgang til de personoplysninger, som de skal bruge i deres arbejde. Adgangsstyring er allerede udvalgt som fokuspunkt af Udvalg for Informationssikkerhed (UFI), som i 2019 vil følge op på regionens systemers efterlevelse af reglerne for adgangskontrol.

Beslutning om cloudstrategi

Brugen af cloud computing (skyen) efterspørges flere steder i regionen. Det forventes, at den kommende digitaliseringsstrategi forudsætter, at der skal laves en cloudstrategi,som skal kridte banen op ift., hvornår og på hvilke vilkår, Region Syddanmark vil benytte cloudtjenester. I denne forbindelse er der udarbejdet et notat med de juridiske risici forbundet med brugen af cloudtjenester. Databeskyttelsesrådgiveren anbefaler, at arbejdet med cloudstrategien fortsat prioriteres højt, og at der som led i strategiarbejdet tages stilling til de databeskyttelsesretlige risici.

Region Syddanmark
Mia Bekker Leimand
Damhaven 12 . 7100 Vejle
Tlf. 2964 9918

regionsyddanmark.dk

15959 - Grafisk Service, Region Syddanmark - 02.2019

Region Syddanmark