

REFERAT Informationssikkerhedsudvalget d. 18-11-2019

Mødedato Mandag d. 18. november 2019 kl. 10:30

Mødested Bogense Rådhus, Mødelokale 1

Indholdsfortegnelse

Samarbejde med Anders Ganer.....	3
Tilsyn med databehandleraftaler.....	5
Living document.....	7
Persondataforordningen - sådan behandler vi persondata om dig.....	8
Gensidig orientering.....	9

Punkt 1: Samarbejde med Anders Ganer

Sagsfremstilling

1. Samarbejde med Anders Ganer

Åbent

Sagsnr. 480-2019-21798 Dok.nr. 480-2019-218285

Sagens kerne

Drøftelse af tre opgaver, som kan løses i samarbejde med ekstern konsulent, Anders Ganer. Opgaverne er:

- Formel model til risikovurdering, som alle kan bruge
- Kontrol med autorisation
- Opbevaring og deling af billeder

Indstilling

Informationssikkerhedsudvalget drøfter opgaverne med Anders Ganer og beslutter, om der skal indledes et samarbejde.

Sagens baggrund

På baggrund af sidste møde i Informationssikkerhedsudvalget den 30. sep. 2019, skal følgende tre opgaver løses:

En formel model til risikovurdering, som alle kan anvende

Der kan med fordel udarbejdes en bred generisk model til risikovurdering, som kan anvendes til såvel It-systemer som andre systemer i kommunen.

Kontrol med autorisationer

Der er nedsat en gruppe i forhold til implementering af den ny version af IDM, som gennemgår samtlige brugerautorisationer, fjerner alle de gamle autorisationer, og danner nogle nye autorisationer. Som en del af opgaven skal der laves en styringsmodel.

Opbevaring og deling af billeder

Det er som følge af drøftelser i hhv. chefgruppen og MED-system aftalt, at Informationssikkerhedsudvalget skal udarbejde et bud på, hvordan vi som kommune fremover håndterer opbevaring og deling af billeder inden for GDPR-lovgivningens rammer.

Økonomiske oplysninger

Sagen har ikke været forelagt Økonomi og Løn.

Lovgrundlag

GDPR-lovgivningen.
Databeskyttelsesloven.
Datatilsynets praksis.

Beslutning

Informationssikkerhedsudvalg den 18. november 2019

Fraværende: Ingen

Ad 1. Formel model for risikovurdering

Det blev besluttet, at data-/systemejere samles til et arbejds møde, hvor resultatet skal være udarbejdelse af risikovurderinger af de forskellige systemer. Forinden laves en skabelon, som tager afsæt i de allerede udarbejdede risikovurderinger for Nexus, Opus, Nova.

Der orienteres om processen på chefgruppemødet i december 2019. Arbejds mødet planlægges til afholdelse i forlængelse af chefgruppemødet i januar 2020.

Anders Ganer udarbejder skabelonen, så den kan vedlægges chefgruppens dagsorden i december 2019.

For at styrke og understøtte arbejdet med riskovurderinger opstartes vurderinger på systemer Momentum, DUBU og Aula som pilotprojekter.

Derudover udarbejdes en risikovurdering ved sletning af data, herunder en vurdering af tidsfrister mv. Et oplæg udarbejdes af Anders Ganer i samarbejde med IT.

Ad 2. Kontrol med autorisation

Anders Ganer udarbejder et årshjul, som kan bruges til at afdække behovet. Kontroller indarbejdes i videst mulig udstrækning i allerede etablerede procedurer og kontroller, fx ledelsestilsynet.

På næste møde drøftes ledelsestilsynet. Gitte Clemmensen fremlægger det nuværende tilsyn.

Ad 3. Opbevaring og deling af billeder

Anders Ganer udarbejder i samarbejde med Strategi og Politik et oplæg.

Supplerende undersøges mulighederne for at udarbejde en pixi-bog til formidling af formål, roller og ansvar i informationssikkerhedsarbejdet, hvor målgruppen er både medarbejdere og ledere.

Punkt 2: Tilsyn med databehandleraftaler

Sagsfremstilling

2. Tilsyn med databehandleraftaler

Åbent

Sagsnr. 480-2019-18968 Dok.nr. 480-2019-189045

Sagens kerne

Tilsyn med kommunens indgåede databehandleraftaler.

Indstilling

Forelægges til drøftelse.

Sagens baggrund

Ifølge Datatilsynet skal kommunen som dataansvarlig påse behandlingssikkerheden hos sine databehandlere, for at leve op til GDPR's krav om ansvarlighed. Det betyder, at kommunen må føre tilsyn med, at databehandleraftaler overholdes, herunder at databehandleren har gennemført de aftalte tekniske og organisatoriske sikkerhedsforanstaltninger.

Kommunen skal kunne dokumentere, at tilsynet er ført. Se nærmere herom i Datatilsynets vejledning om tilsyn med databehandlere: <https://www.datatilsynet.dk/media/6865/vejledende-tekst-om-tilsyn-med-databehandlere-og-underdatabehandlere.pdf>, hvor det bl.a. er eksemplificeret hvorledes kontrol med databehandlere kan føres i praksis (se side 4).

I kommunens standarddatabehandleraftale er følgende bestemt herom, jf. pkt. 10:

10.2 Kommunen, en repræsentant for Kommunen eller dennes revision (såvel intern som ekstern) har adgang til at foretage inspektioner og revision hos Leverandøren, få udleveret dokumentation, herunder logs, stille spørgsmål m.v. med henblik på at konstatere, at Leverandøren overholder de krav, der følger af denne Aftale.

10.3 Leverandøren skal én gang årlig vederlagsfrit til Kommunen fremsende en erklæring om overholdelse af denne Aftale. Erklæringen skal udarbejdes i overensstemmelse med gældende, anerkendte branchestandarder på området, og skal omfatte både Leverandørens og eventuelle underdatabehandlers databehandling. Den første erklæring skal foreligge 12 måneder efter Hovedaftalens indgåelse.

Alle system- og dataansvarlige (som udgangspunkt niveau 2 eller 3 chef/leder, registreret centralt i KITOS) skal derfor sikre sig, at der til den aftalte frist hvert år modtages erklæringer som aftalt i henhold til samtlige databehandleraftaler indenfor eget område, og yderligere sikre sig, at erklæringerne er fyldestgørende, og i modsat fald foretage det relevante i anledning heraf. Er en konkret databehandleraftale formuleret anderledes end angivet ovenfor, enten fordi formuleringen i standardaftalen er blevet fraveget eller fordi den aftale, der er indgået, ikke er baseret på kommunens standarddatabehandleraftale, er det den konkrete formulering, der skal påses overholdt i overensstemmelse med GDPR og Datatilsynets vejledning.

Informationssikkerhedsudvalget drøfter, om ovennævnte giver anledning til tiltag, for eksempel intern kontrol, systematisk indberetning til f.eks. DPO, awarenesskampagner eller andet.

Økonomiske oplysninger

Sagen har ikke været forelagt Økonomi og Løn.

Lovgrundlag

Databeskyttelsesforordningens artikel 28 samt artikel 32.

Beslutning

Informationssikkerhedsudvalg den 30. september 2019

Fraværende: Ingen

Økonomi undersøger, om de dataansvarliges tilsyn med databehandleraftaler kan indbygges i ledelsestilsynet i forbindelse med regnskabsafslutningen, så ledelsestilsynet på databehandleraftalerne kommer ind i en fast rutine.

Punktet optages på næste møde som beslutningspunkt.

Beslutning

Informationssikkerhedsudvalg den 18. november 2019

Fraværende: Ingen

Indarbejdes i ledelsestilsynet, hvor Gitte Clemmensen præsenterer et forslag på næste møde.

Punkt 3: Living document

Sagsfremstilling

3. Living document

Åbent

Sagsnr. 480-2018-17097 Dok.nr. 480-2019-205646

Sagens kerne

Informationssikkerhedsudvalgets "Living document" viser, hvad der har været arbejdet med siden sidst.

Indstilling

Forelægges til orientering.

Sagens baggrund

Informationssikkerhedsudvalgets "Living document" viser, hvad der har været arbejdet med siden sidst.

Økonomiske oplysninger

-

Lovgrundlag

-

Bilag

480-2019-205648 Living document 2018/2019 - rev. november 2019

Beslutning

Informationssikkerhedsudvalg den 18. november 2019

Fraværende: Ingen

Orientering foretaget.

Bilag

Living document 2018/2019 - rev. november 2019

Punkt 4: Persondataforordningen - sådan behandler vi persondata om dig

Sagsfremstilling

4. Persondataforordningen - sådan behandler vi persondata om dig Åbent

Sagsnr. 480-2019-25355 Dok.nr. 480-2019-215681

Sagens kerne

I forbindelse med persondataforordningen er det et krav at arbejdsgiveren oplyser medarbejderne om, hvilke data der registreres om dem og hvordan de bruges.

På grundlag af vejledning fra KL har Økonomi og Løn udarbejdet kladde til dette brev, som forelægges til drøftelse.

Indstilling

Det indstilles, at kladde til brev til alle medarbejdere drøftes.

Sagens baggrund

I forbindelse med persondataforordningen er Nordfyns Kommune som arbejdsgiver forpligtet til at fortælle den enkelte medarbejder, hvilke data der registreres om den enkelte medarbejder.

Økonomi og Løn har afventet, at KL udsendte en vejledning omkring emnet og denne vejledning blev modtaget i foråret 2019.

Der er udarbejdet en kladde til brev til samtlige medarbejdere som fremsendes til orientering og kommentering.

Tidsplan

18.11 Brevet drøftes i Informationssikkerhedsudvalget

19.11 Brevet drøftes i HovedMED

04.12 Direktionen godkender endelig formulering

Medio dec. Brevet sendes til alle medarbejders e-boks

Fremover vil alle medarbejdere via ansættelsesbrevet blive anmodet om på intranettet at læse, hvad der registreres om den enkelte medarbejder.

Økonomiske oplysninger

-

Lovgrundlag

Persondataforordningen.

Bilag

480-2019-214901 Sådan behandler vi personoplysninger om dig

Beslutning

Informationssikkerhedsudvalg den 18. november 2019

Fraværende: Ingen

Godkendt.

Bilag

Sådan behandler vi personoplysninger om dig

Punkt 5: Gensidig orientering

Sagsfremstilling

5. Gensidig orientering

Åbent

Sagsnr. 480-2019-21798 Dok.nr. 480-2019-205645

Sagens kerne

Gensidig orientering.

Indstilling

Forelægges til orientering.

Sagens baggrund

-

Økonomiske oplysninger

Sagen har ikke været forelagt Økonomi og Løn.

Lovgrundlag

Intet.

Beslutning

Informationssikkerhedsudvalg den 18. november 2019

Fraværende: Ingen

Orientering foretaget.