REFERAT Informationssikkerhedsudvalget d. 30-09-2019

Mødedato Mandag d. 30. september 2019 kl. 14:00

Mødested Bogense Rådhus, Mødelokale 1

Indholdsfortegnelse

Punkt 1: Dataminimering og slettefrister

Sagsfremstilling

1. Dataminimering og slettefrister Åbent

Sagsnr. 480-2019-16677 Dok.nr. 480-2019-139013

Sagens kerne
Dataminimering og slettefrister.

Indstilling
Forelægges til drøftelse.

Sagens baggrund
Det fremgår af GDPR artikel 5, stk. 1, litra c), at personoplysninger skal være begrænset til, hvad der er nødvendigt i forhold til de formål, hvortil de behandles.

Dette er udtryk for et grundlæggende princip om dataminimering. Princippet indebærer blandt andet, at kommunen skal forholde sig til sletning af data i form af personoplysninger, herunder slettefrister, sletterutiner, selve sletningen og dokumentation herfor.

Det fremgår af GDPR artikel 5, stk. 2, at den dataansvarlige er ansvarlig for og skal kunne påvise, at stk. 1 overholdes. At kommunen skal kunne påvise, at bl.a. princippet om dataminimering overholdes betyder, at man skal have dokumentation for, at man har de rigtige slettefrister og sletterutiner, og at man har udført selve sletningen af data. Det er altså ikke nok i sig selv, at man sletter korrekt, hvis man ikke kan bevise, at man sletter korrekt. Bevisbyrden påhviler kommunen.

Et konkret eksempel på dokumentation kan være en protokolført beslutning med oplistning af vejledende slettefrister inden for f.eks. et direktørområdes forskellige sagsområder. Beslutningen skal selvfølgelig være fulgt op således, at slettefristerne også anvendes i praksis.

Af GDPR artikel 30, stk. 1, litra f) fremgår, at hver dataansvarlig fører fortegnelser over behandlingsaktiviteter under deres ansvar, der skal omfatte oplysninger om, hvis det er muligt, de forventede tidsfrister for sletning af de forskellige kategorier af oplysninger. Det betyder, at kommunen som dataansvarlig skal foretage en vurdering af, hvor længe indsamlede oplysninger skal opbevares, og opfylde kravet om at angive slettefristerne.

Bemærk, at KLE bidrager til at understøtte kravet om forventede tidsfrister for sletning, idet alle emneområder i KLE, hvor det antages, at der kan indgå personoplysninger, nu er knyttet sammen med en anbefalet tidsfrist for sletning. Se KLE online her:
http://www.kle-online.dk/emneplan/00/

I den forbindelse henledes udvalgets opmærksomhed på, at når man i Nordfyns Kommune opretter en sag, hvor KLE's anbefalede tidsfrist er for eksempel 5 år, da kan det forekomme at sagen er tilgængelig i en periode på for eksempel 10 eller 30 år efter sagens afslutning. Dette er problematisk, særligt da Nordfyns Kommunes fortegnelser over behandlingsaktiviteter generelt henviser til KLE's anbefalede slettefrister.

Et eksempel på ovenstående problemstilling er KLE sagstype nummer 00.07.03, partens aktindsigt, hvor KLE's anbefalede slettefrist er 5 år, men en KMD-sag oprettet i dette KLE nummer i Nordfyns Kommune er tilgængelig i 30 år efter afslutning, medmindre man aktivt og manuelt ændrer dette i forbindelse med oprettelsen. Et andet eksempel er KLE sagstype 84.00.00, offentlige valg, hvor KLE's anbefalede frist er 5 år, men kommunens sager er tilgængelige i 10 år.

Et af Datatilsynets fokusområder for øjeblikket er sletning af data i kommunerne, da Datatilsynet har konstateret, at dette område, særligt selve sletningen samt imødekommelsen af de store dokumentationskrav, lader meget tilbage at ønske i kommunerne.

På baggrund heraf drøfter udvalget Nordfyns Kommunes sletning af personoplysninger.

Økonomiske oplysninger
Sagen har ikke været forelagt for Økonomi og Løn.

Lovgrundlag
GDPR artikel 5 og 30.

Beslutning
Informationssikkerhedsudvalg den 30. september 2019
Fraværende: Ingen

Strategi og Politik forbereder punktet til beslutning på næste møde med udgangspunkt i følgende;
- KLEs vejledning til slettefrister følges.
- Kommunikation til organisationen med fokus på de digitale ambassadører omkring vigtigheden i korrekte slettefrister ved oprettelse af sager.

Strategi og Politik undersøger endvidere mulighederne for at makulere/destruere papirarkiverne på rådhusene med henblik på at sikre overholdelse af slettefristerne, hermed også at styrke indsatsen i informationssikkerheden.

Punkt 2: Tilsyn med databehandleraftaler

Sagsfremstilling

2. Tilsyn med databehandleraftaler Åbent

Sagsnr. 480-2019-18968 Dok.nr. 480-2019-160762

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.datatil synet.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 underdatabehandleres 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 forindelse med regnskabsafslutningen, så ledelsestilsynet på databehandleraftalerne kommer ind i en fast rutine.

Punktet optages på næste møde som beslutningspunkt.

Punkt 3: Deling og opbevaring af billeder

Sagsfremstilling

3. Deling og opbevaring af billeder Åbent

Sagsnr. 480-2019-18986 Dok.nr. 480-2019-160790

Sagens kerne
Deling og opbevaring af billeder i overensstemmelse med GDPR.

Indstilling
Forelægges til drøftelse.

Sagens baggrund
Billeder karakteriseres som personoplysninger, og behandling af billeder skal derfor ske i overensstemmelse med databeskyttelsesforordningens regler, særligt opfylde behandlingsprincipperne i forordningens art. 5.

Opbevaring af billeder
Når billeder opbevares er der tale om behandling af personoplysninger, og dette skal bl.a. ske efter princippet om god databehandlingsskik, jf. art. 5, stk. 1, litra a. Dette indebærer, at billederne opbevares på en lovlig, rimelig og gennemsigtig måde. Særligt skal billederne opbevares med et lovligt formål og med hjemmel hertil. Ligeledes skal billederne opbevares sikkert, jf. art. 5, stk. 1, litra f, hvilket indebærer at kommunen skal sikre, at billeder opbevares således, at uvedkommende ikke kan få adgang til billederne.

Formålet, som billederne tages og opbevares til, skal være sagligt og billederne må ikke anvendes til et andet formål end det, de er taget til (formålsbestemthed), med mindre der gives samtykke hertil fra de(n) registrerede på billedet, jf. art. 5, stk. 1, litra b. Et eksempel herpå kan være billeder, der er taget af skolebørn på en lejrtur til internt brug i klassen eller lign., så må billederne ikke bruges til markedsføring af lejrturen næste gang uden samtykke.

Kommunen skal på baggrund af behandlingsprincipperne i art. 5 sikre, at billeder opbevares på sikker og forsvarlig vis – eksempelvis ved at de ikke opbevares på private telefoner, eller at der f.eks. er et organiseret, sikkert system til opbevaring af billeder. Tillige skal der opmærksomhed på, at billeder alene tages og opbevares til et sagligt formål, eksempelvis identifikation af elever eller collage af en lejrtur.

Offentliggørelse og deling af billeder
Hvis billeder er taget og opbevares med henblik på intern brug, må disse ikke offentliggøres på en hjemmeside efterfølgende foruden samtykke. Ved indhentelse af samtykke skelnes der imellem situationsbilleder, situationsbilleder der kan være krænkende/udstillende eller portrætbilleder. Situationsbilleder (f.eks. børn der leger i en skolegård) kan offentliggøres uden samtykke, hvor situationsbilleder, der kan være krænkende samt portrætbilleder kræver samtykke førend de lovligt kan deles eller offentliggøres. Se mere om offentliggørelse af billeder på Datatilsynets hjemmeside: https://www.datatilsynet.dk/emner/internet-og-apps/billeder-paa-internettet/

Det skal haves for øje, at såfremt der er tale om billeder af børn og unge, at denne gruppe af registrerede nyder en særlig beskyttelse, og at der skal indhentes samtykke fra forældremyndighedsindehaver, hvis barnet er under 16 år.

Informationssikkerhedsudvalget drøfter, om der skal udarbejdes en politik for håndtering af billeder, udstikkes retningslinjer herfor eller på anden måde skabes opmærksomhed på området.

Økonomiske oplysninger
Sagen har ikke været forelagt Økonomi og Løn.

Lovgrundlag
Databeskyttelsesforordningens art. 5.

Beslutning
Informationssikkerhedsudvalg den 30. september 2019

Fraværende: Ingen

GDPR betyder store udfordringer i forhold til at tage fotos af borgerne, når de færdes i/bruger vores institutioner. Udfordringerne er blandt andet:

- Borgernes ret til at blive slettet gælder også fotos
- Hvis borgere trækker en accept af fotografering tilbage, så skal fotos med borgeren slettes
- Fotos må kun bruges til det formål, de blev taget til.
- Fotos må ikke tages med private telefoner mv.
- Fotos skal opbevares som andre personfølsomme data, det betyder i realiteten i NOVA.

Brugen og delingen af fotos og video er blevet en vigtig del af samspillet mellem pårørende/forældre og institutionerne. Det er værdsat af de pårørende/forældrene, at man kan følge lidt med i livet på plejecentrene, i daginstitutionerne og i skolerne.

Derfor er der et dilemma i forhold til at GDPRs krav til behandling af persondata og de pårørendes/forældrenes ønsker og forventninger.

Dilemmaet drøftes på det kommende chefmøde.

Punkt 4: Opdatering af tekst mv. på intranettet

Sagsfremstilling

4. Opdatering af tekst mv. på intranettet Åbent

Sagsnr. 480-2019-20830 Dok.nr. 480-2019-176297

Sagens kerne
Rettelser og præciseringer til dele af teksterne, der ligger under punktet "Informationssikkerhed" på intranettet.

Indstilling
Forelægges til drøftelse.

Sagens baggrund
Efter GDPR trådte i kraft for knapt halvandet år siden, har det vist sig, at der på intranettet er behov for en ajourføring af informationen til kommunens medarbejdere. Det har bl.a. vist sig, at nogle retningslinjer (særligt i forbindelse med databehandleraftaler) er uhensigtsmæssige i den daglige drift.

Derfor foreslås følgende præciseringer, således at DPO'ens opgaver bliver lettede og teksten er i overensstemmelse med behovet for vejledning.

Databehandleraftaler
Link til undersiden: https://intranet.nordfynskommune.dk/Om-kommunen/Informationssikkerhed/Databehandleraftale

Rettelser til "Procedure for indgåelse af databehandleraftale":
· Proceduren er ikke opdateret, da der står, at en vejledning til indgåelse af databehandleraftaler er under udarbejdelse.
· Derudover er det misvisende, at der er opremset følsomme personoplysninger, da en databehandleraftale er relevant så snart der behandles personoplysninger (både almindelige og følsomme) på vegne af kommunen.
· Det er anført, at DPO'en kan godkende databehandleraftalerne, og dette bør ændres, således der anføres, at der kan søges rådgivning hos DPO'en eller juristerne, såfremt der er spørgsmål til indgåelse af databehandleraftale.
Vejledning til årligt tilsyn med databehandlere:
· En uddybende vejledning til hvordan den systemansvarlige kan udføre tilsyn med databehandlere bør tilføjes – dette med afsæt i Datatilsynets vejledning herom: https://www.datatilsynet.dk/media/6865/vejledende-tekst-om-tilsyn-med-databehandlere-og-underdatabehandlere.pdf

Digitalt kodeks
Link til undersiden: https://intranet.nordfynskommune.dk/Om-kommunen/Informationssikkerhed/Haandbog

Præcisering til afsnittet "Jeg går ind for genbrug af data. Det medfører, at…":
· Det fremgår, at der opfordres til at data skal deles med så mange som muligt. Dette virker misvisende, da data ikke bør deles i flæng – ej heller selvom den skal være tilgængelig og mulig at tilgå for andre. Sætningen bør slettes.

Økonomiske oplysninger
Sagen har ikke været forelagt Økonomi og Løn.

Lovgrundlag
GDPR.

Beslutning
Informationssikkerhedsudvalg den 30. september 2019
Fraværende: Ingen

Godkendt.

Punkt 5: Living document

Sagsfremstilling

5. Living document Åbent

Sagsnr. 480-2018-17097 Dok.nr. 480-2019-160742

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

480-2019-160755 Living document 2018/2019 - rev. september 2019

Beslutning
Informationssikkerhedsudvalg den 30. september 2019
Fraværende: Ingen

Orientering foretaget.

Bilag

Living document 2018/2019 - rev. september 2019

Punkt 6: Høring - Kortlægning af dataplaceringskrav, jf. Forordningen for frie datastrømme

Sagsfremstilling

6. Høring - Kortlægning af dataplaceringskrav, jf. Forordningen for frie datastrømme Åbent

Sagsnr. 480-2019-17761 Dok.nr. 480-2019-185817

Sagens kerne
Høring – Kortlægning af dataplaceringskrav, jf. Forordningen for frie datastrømme.

Indstilling
Forelægges til drøftelse.

Sagens baggrund
Erhvervsstyrelsen er udpeget som nationalt kontaktpunkt og vil forestå kontakten omkring dataplaceringskravene til Europa-Kommissionen.
I første omgang skal der ske en kortlægning af alle eksisterende dataplacerings-krav som findes i danske love og administrative bestemmelser af generel karakter, som eksempelvis bekendtgørelser.

I bedes senest den 1. oktober 2019 udfylde og returnere vedlagte skema med angivelse af eksisterende dataplaceringskrav i danske love, bekendtgørelser og administrative bestemmelser af generel karakter indenfor egne ressortområ-der. Skemaet skal sendes til sopvas@erst.dk og metgod@erst.dk.

Ophævelse af dataplaceringskrav
Eksisterende dataplaceringskrav, som ikke kan begrundes i hensynet til offentlig sikkerhed og samtidig er i overensstemmelse med proportionalitetsprincippet, skal ophæves senest 30. maj 2021, jf. forordningens art. 4, stk. 3. ***Det er det enkelte ministeriums ansvar at sørge for, at dataplaceringskravene på eget res-sortområde ophæves inden for fristen.***

Økonomiske oplysninger
Sagen har ikke været forelagt Økonomi og Løn.

Lovgrundlag
-

Bilag

480-2019-185814	EU-Kommissionens vejledning
480-2019-185813	Forordning om frie datastrømme
480-2019-185812	Information om forordningen om frie datastrømme - Regioner og Kommuner
480-2019-185811	Skema til udfyldelse
480-2019-185810	Høringsbrev ang. kortlægning af dataplaceringskrav jf. Forordningen for frie datastrømme

Beslutning

Informationssikkerhedsudvalg den 30. september 2019
Fraværende: Ingen

Orientering foretaget.

Bilag

EU-Kommissionens vejledning

Forordning om frie datastrømme

Information om forordningen om frie datastrømme - Regioner og Kommuner

Skema til udfyldelse

Høringsbrev ang. kortlægning af dataplaceringskrav jf. Forordningen for frie datastrømme

Punkt 7: Gensidig orientering

Sagsfremstilling

7. Gensidig orientering Åbent

Sagsnr. 480-2019-21798 Dok.nr. 480-2019-184461

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 30. september 2019
Fraværende: Ingen

Følgende blev drøftet:

Anders Ganer inviteres til næste møde med henblik på at arbejde videre med yderligere tiltag. Forslag fra Anders er:
- Formel model til risikovurdering, som alle kan bruge.
- Kontrol med autorisation.

Skal der arbejdes videre med et tilbud til institutionerne om at de kan få et "uvildigt" GDPR-tjek, hvis de ønsker det?

Det overvejes, hvordan der kan følges op på GDPR-bevidstheden ved medarbejderne. Flere kommuner har købt eksterne systemer, som via spørgeskemaer/e-Learning undersøger organisationens awareness niveau. Strategi og Politik undersøger, om det evt. kan indgå i trivselsundersøgelsen med få og korte spørgsmål.

Det blev drøftet, om en inspirationstur til andre kommuner kunne være med til at udvikle Informationssikkerhedsudvalgets arbejde. Drøftes nærmere.