REFERAT Informationssikkerhedsudvalget d. 03-02-2023

Mødedato	Fredag d. 03. februar 2023 kl. 08:30
Mødested	Bogense Rådhus
Mødedeltagere	Tina Wrøbel, Per Stenaa, Gitte Clemmensen, Birgit Mia Larsson, Vicki Møberg Torp

Indholdsfortegnelse

Tidsplan..... 3
Brug af kommunale enheder i Nordfyns Kommune..... 4
Lukning af U-drev, godkendelse af nye retningslinjer for tværfaglig deling af dokumenter..... 6
Implementering af beredskabsplan i Nordfyns Kommune..... 8
GDPR Awarenes 2023..... 9
DPO Årsberetning 2022..... 11

Punkt 1: Tidsplan

S2021-739

Sagens kerne

Tidsplan

Kl. 13:30 - 13:35	Godkendelse af tidsplan
Kl. 13:35 - 13:55	Brug af kommunale enheder i Nordfyns Kommune
Kl. 13:55 - 14:15	Lukning af U-drev, godkendelse af Retningslinjer for tværfaglig deling af dokumenter
Kl. 14:15 - 14:30	Implementering af beredskabsplan i Nordfyns Kommune
Kl. 14:30 - 14:40	GDPR awarenes 2023
Kl. 14:40 - 14:50	DPO Årsrapport 2022
Kl. 14:50 - 15:00	Eventuelt

Beslutning

Godkendt.
Med forbehold for, at mødet er flyttet til anden dato og tidspunkt på dagen.

Punkt 2: Brug af kommunale enheder i Nordfyns Kommune

S2021-19067

Sagens kerne

Informationssikkerhedsudvalget drøfter vægtningen af teknisk sikkerhed forbundet med brug af Kommunale enheder, overfor organisatoriske hensyn som rekruttering og fastholdelse, smidig opgaveløsning og bæredygtighed.

Indstilling

Informationssikkerhedsteamet indstiller, at Informationssikkerhedsudvalget enten:
1. Godkender vedlagte retningslinjer for brug af kommunale enheder
eller
2. Anviser hvilke ændringer, der ønskes implementeret i retningslinjerne, med henblik på endelig godkendelse på næste møde.

Sagens baggrund

På Informationssikkerhedsudvalgsmødet den 9. november 2021 afgav DPO anbefalinger til, hvordan Nordfyns Kommune bør anvise de ansatte at anvende digitale kommunale enheder. Anbefalingerne lød som følger:

- Teknisk adskillelse af arbejdsmæssig og privat brug af kommunale smartphones og tablets, hvorved privat brug vil kunne fortsætte uden forøget risiko for fejl

alternativt

- Ophører med at tillade privat brug af kommunalt ejede smartphones

Udvalget ønskede på denne baggrund mulighed for at drøfte anbefalingerne sat op imod organisatoriske hensyn, så som fastholdelse og rekruttering, smidige arbejdsgange (mindre bøvl) og bæredygtighed.

Vurdering af sammenhængen:
De tre hensyn, som informationssikkerhedsudvalget ønsker at prioritere sikkerhedsniveauet op imod er alle sammen legitime kommunale hensyn. Det vurderes ligeledes, at særligt to af de tre hensyn vil blive påvirket negativt, hvis anbefalingerne fra DPO om ikke at tillade privat brug af kommunale enheder følges. Det vurderes, at de ansatte som i dag er van til at kunne anvende kommunale enheder privat, vil opleve det som bøvlet og mindre attraktivt, hvis denne adgang forsvinder, og det er sandsynligt, at beslutningen kan have en negativ effekt ift. ansøgere til stillinger i kommunen.

Det i et bæredygtighedsmæssigt perspektiv, vil en beslutning om ikke at tillade privat brug af kommunale enheder betyde, at mange vil erhverve sig en enhed privat. Dermed medfører en sådan beslutning et øget forbrug af devices, hvilket påvirker miljø og klima negativt.

Den alternative anbefaling om at sikre teknisk adskillelse af arbejdsmæssig og privat brug anslås at koste minimum 350.000 kr. årligt. Der forventes ikke at medfølge vedvarende negative konsekvenser i forhold til fastholdelse og rekruttering, smidige arbejdsgange eller bæredygtighed som følge af den model.

Ovenstående betragtninger bør ligeledes perspektiveres op imod, at der ikke tidligere er konstateret sikkerhedsbrud som følge af, at medarbejderne har mulighed for at anvende kommunale enheder privat. Summen af betragtningerne afvejes af Informationssikkerhedsudvalget i den risikovurdering, som Informationssikkerhedsudvalget lægger til grund for godkendelsen af Retningslinjer for brug af kommunale enheder.

Økonomiske oplysninger

Ikke relevant på nuværende tidspunkt

Lovgrundlag

Persondataforordningen

Beslutning

Informationssikkerhedsudvalget drøftede brug af kommunale enheder i Nordfyns Kommune og forslag til retningslinjer med følgende input:

- Muligheden for brug af to simkort er ikke en velegnet løsning til at styre privat og arbejdsmæssig brug

- tydelig kommunikation og udfoldelse af, hvordan man kan og må bruge enhederne, med henblik på at minimere risikoen for fejl.
- Løbende orientering om korrekt brug som en del af GDPR-awarenes til alle kommunens medarbejdere.

Eksisterende sikkerhedsopsætning risikovurderes og mitigeres med henblik på efterfølgende godkendelse i Informationssikkerhedsudvalget.

Bilag

Retningslinjer for brug af kommunale enheder

Punkt 3: Lukning af U-drev, godkendelse af nye retningslinjer for tværfaglig deling af dokumenter

S2021-4191

Sagens kerne

Proces for lukning af U-drev drøftes og Retningslinjer for tværfaglig deling af dokumenter godkendes.

Indstilling

Informationssikkerhedsteamet orienteres om proces for lukning af U-drevet, og godkender Retningslinjer for tværfaglig deling af dokumenter

Sagens baggrund

I 2022 blev der konstateret et sikkerhedsbrud som allerede ved konstateringen var 2 år gammelt. Bruddet bestod i, at der var gemt personfølsomme oplysninger på U-drevet, som alle ansatte dermed havde uhindret adgang til at læse.
Det konstaterede sikkerhedsbrud er nu løst, men der er overordentlig mange andre oplysninger på U-drevet, som der ikke er opsyn med, hvorfor der potentielt kan findes flere sikkerhedsbrud. Der er nu udarbejdet en retningslinje for, hvordan fagområderne skal gøre fremadrettet, når der skal ske deling af dokumenter mellem fagområderne.

Proces for lukning af U-drevet
Når Retningslinjer for tværfaglig deling af dokumenter er godkendt af Informationssikkerhedsudvalget, skal de implementeres i fagområderne. Dette sker i tæt samarbejde med Organisation og HR. I forbindelse med denne implementering, vil fagområderne blive instrueret i at flytte alle de dokumenter, som fortsat skal deles mellem fagområder, væk fra U-drevet og over på de løsninger, som passer til delingens formål, jf. retningslinjerne.

Dette arbejde må forventes af tage tid. Ikke desto mindre er hver dag der går med den nuværende opsætning af U-drevet en potentiel sikkerhedsrisiko. Det er derfor nødvendigt med en drøftelse af, hvor lang en frist Nordfyns Kommune kan acceptere, set i forhold til den risiko, som den nuværende løsning repræsenterer. Denne drøftelse bør foretages i Direktionen, med henblik på at forpligte direktørerne på både ansvaret for opgaven og den fremadrettede løsning.
Anbefalingen er, at sagen drøftes ledelsesmæssigt i februar 2023 og at opgave håndteres i marts, med henblik på endelig lukning af U-drevet senest 31. marts 2023.

Processkridt:
1. godkendelse af retningslinjer
2. planlægning af implementering af retningslinjer (Informationssikkerhedsteam samt Organisation og HR)
3. drøftelse i Direktionen i februar 2023
4. implementering i marts 2023 jf. drøftelser i Direktionen.
5. lukning af U-drev 31. marts 2023

Økonomiske oplysninger

ikke relevant

Lovgrundlag

Persondataforordningen

Beslutning

Orientering foretaget.
Procesplanen skal revideres og forelægges direktionen den 22. februar 2023
Procesplanen skal imødekomme fagområdernes behov for alternative løsninger, herunder også en orientering om, at medarbejderne mister adgang til U-drevet den 30. april 2023.
Data på U-drevet gemmes i en afgrænset periode og kan derfor stadig findes frem ved konkret behov. Kommunikation inddrages i formidlingen af ovenstående til organisationen.

Bilag

Retningslinjer for tværfaglig deling af dokumenter.

Punkt 4: Implementering af beredskabsplan i Nordfyns Kommune

S2022-26328

Sagens kerne

Beredskabsplanen forelægges til drøftelse i forhold til implementering.

Indstilling

Informationssikkerhedsteamet indstiller, at Informationssikkerhedsudvalget drøfter, hvordan beredskabsplanen implementeres I Nordfyns Kommune.

Sagens baggrund

Vedhæftede beredskabsplan er udarbejdet i sin grundform i 2020, i samråd med et fynsk fællesskab (de fynske It-chefer og informationssikkerhedsprofiler, samt ATEA)
Informationssikkerhedsudvalget skal drøfte om beredskabsplanen evt. skal tilrettes Nordfyns Kommunes sprog og begreber, og hvordan den implementeres bedst muligt i organisationen, herunder også hvor det fremadrettede ansvar for kontrollen hermed skal forankres.

Udover at omhandle almindelig håndtering af I-sikkerhed, er det ligeledes et NSIS krav, at en sådan plan er godkendt, implementeret, efterlevet og testes årligt.

Økonomiske oplysninger

Ikke relevant.

Lovgrundlag

Informationssikkerhed generelt og NSIS krav i særdeleshed

Beslutning

Drøftet.

Informationssikkerhedsudvalget godkender beredskabsplanen med følgende kommentarer:
- Tydeliggør, hvilken sammenhæng og hvilke snitflader den har til andre beredskabsplaner i kommunen.
- Beskriv den organisatoriske support der er til rådighed for IT, når krisen rammer. Dette for at sikre en hensigtsmæssig udnyttelse af tekniske resurser under krisehåndteringen. (Krisestab eller andre supporterende organer).
- Erstat begreber og navne, til Nordfyns Kommune sprog generelt (f.eks. Digitalisering og i-sikkerhed)
- Der skal udarbejdes konkretiserende bilag til den overordnede plan, som har til formål at udmønte indholdet.
- Definer opdatering af planen, så den passer til Nordfyns Kommune, og ligeledes sikrer en smidighed herfor.
- Beredskabsplanen og udmøntning heraf lægges på Informationssikkerhedsudvalgets årshjul.

Ny IT og Digitaliseringsstrategi skal forholde sig til beredskabsplanen og referere til den. Dette for at sikre sammenhæng.

Bilag

Beredskabsplan for IT og Informationssikkerhed - Nordfyns Kommune version 1

Punkt 5: GDPR Awarenes 2023

S2023-167

Sagens kerne

Informationssikkerhedsudvalget drøfter Informationssikkerhedsteamets oplæg til awarenes generelt og for 2023.

Indstilling

Informationssikkerhedsteamet indstiller, at Informationssikkerhedsudvalget godkender planerne for GDPR awarenes.

Sagens baggrund

GDPR awarenes har primært til formål at sikre et passende vidensniveau for alle ansatte i forhold til behandlingen af personoplysninger. Uden et passende vidensniveau stiger risikoen for fejl under behandlingen af borgernes personoplysninger, og dermed også risikoen for, at disse fejl udløser konsekvenser for borgerne.

Det sekundære formål med awarenes er, at sikre dokumentation for at medarbejderne har et passende vidensniveau. Uden denne dokumentation er det ikke muligt for arbejdspladsen at leve op til kravet om "passende organisatoriske foranstaltninger" i forhold til beskyttelse af borgernes personoplysninger, jf. persondataforordningen bestemmelser herom.

Det foreslås derfor, at GDPR awarenes fremadrettet bliver et fast punkt på informationssikkerhedsudvalgets 1. møde hvert år, med henblik på evaluering af det forgangene års indsats og orientering om det planlagte for året der kommer. Dokumentationen herfor sikres ved, at der oprettes en sag i NOVR, som alle GDPR awarenes initiativer dokumenteres på.

Status for Awarenes
I 2021 blev der udrullet en generel GDPR awarenes kampagne i det meste af organisationen. Forventningen var, at resultatet heraf ville kunne afspejle sig direkte i antallet af indberettede sikkerhedsbrud for 2022. Dette viste sig desværre ikke at være tilfældet, selv om der statistisk set burde være mange flere sikkerhedsbrud i en organisation som Nordfyns Kommune. Det er uvist, hvorfor awarenes kampagnen ikke har ført til flere anmeldelser af sikkerhedsbrud. Det er usandsynligt, at det skulle være på grund af et meget højt vidensniveau i organisationen generelt, og det er ligeledes usandsynligt, at det skulle skyldes en markant højere disciplin hos os, end i andre sammenlignelige kommuner. Tilbage står formodningen om, at initiativet ikke har mødt organisationen der, hvor den er, og at der skal andre redskaber til, for at opnå den effekt og dokumentation, som bør være til stede.

Forslag til program for 2023
I erkendelse af ovenstående, er det Informationssikkerhedsudvalgets opfattelse, at Nordfyns Kommune har behov for en anderledes tilgang til forståelsen af GDPR generelt, og at denne forståelse ikke vil kunne opnås ved pålæg om gennemførelse af initiativer, som organisationen ikke forstår nødvendigheden af. Nordfyns Kommune har behov for en mere målrettet tilgang til opgaven således behovet for en forandring giver mening for fagområderne. Dermed sikres ejerskab i forandringsprocessen.

informationssikkerhedsteamet er opmærksomme på, at denne tilgang kan risikere at forlænge omstillingsprocessen yderligere, men er ligeledes opmærksomme op, at det i højere grad vil sikre en vedvarende forandringsproces, hvor risikoen for tilbagefald til gamle vaner må forventes at være mindre.

Informationssikkerhedsteamet foreslår, at den primære kilde til awarenes i 2023 blive udrulning af retningslinjer for arbejdsgange hvor der behandles personoplysninger, og at implementeringen heraf udnyttes til generel awarenes, herunder:

1. Politik for informationssikkerhed
2. retningslinjer for brug af SMS i Nordfyns Kommune

Følgende på vej:
3. brug af kommunale enheder
4. lukning af u-drevet
5. kommunikation med borgere i Nordfyns Kommune.

For at kunne udnytte ovenstående og kommende udrulninger af retningslinjer og arbejdsgange til GDPR awarenes, forudsætter det en høj grad at kommunikation med de ansatte. Dette skal først og fremmest ske via intranettet, men det er

også nødvendigt med en højere grad at dialog og orientering i ledelsesstregen samt i MED organisationen. Uden forståelse og ejerskab i organisationen generelt vil den nødvendige effekt endnu en gang udeblive.

På baggrund af ovenstående vil DPO planlæge en besøgsrunde hos fagchefer og I MED-udvalg i efteråret 2023, med henblik på dialog om fagområdernes konkrete vidensniveau, forandringsprocessen i forhold hertil og eventuelle behov i denne anledning. Fagchefernes input vil blive drøftet på inforationssikkerhedsudvalgets første møde i 2024, jf. årshjulet for awarenes.

Informationssikkerhedsteamet er opmærksomme på, at ovenstående metode ikke imødekommer kravene for awarenes og dokumentation på medarbejder niveau. En ny kampagne målrettet dokumentation på medarbejder niveau foreslås derfor planlagt i ultimo 2023.

Økonomiske oplysninger

Punktet har ikke været forelagt Økonomi og Løn.

Lovgrundlag

Persondataforordningen.

Beslutning

Godkendt, med nedenstående bemærkninger.

Samtidighed i forhold til udrulning af initiativer og DPO besøg i organisationen kan skabe gode synergier. Der opleves til tider tvivl i organisationen om, hvad awarenes er, og hvem der har opgaven. Det element tager DPO med ud til afdelingerne.
Andre fagområder kan med fordel anvende awarenes-LOG sagen i NOVA til dokumentation af lokale tiltag.

Punkt 6: DPO Årsberetning 2022

S2023-910

Sagens kerne

Informationssikkerhedsudvalget orienteres om DPO Årsberetning 2022.

Indstilling

DPO indstiller, at informationssikkerhedsudvalget tager DPO årsberetning 2022 til efterretning.

Sagens baggrund

DPO i Nordfyns Kommune udarbejder hvert år en beretning, hvori der gives en generel status på arbejdet med behandling af personoplysninger i Nordfyns Kommune, og en status på det forgangne års igangsatte og gennemførte initiativer i organisationen.

Forventningen til 2022 fra sidste årsberetning var:

- implementering af et organisationssystem, som skal sætte opgaver med persondatabehandling i system og procesunderstøtte arbejdet samt give ledelsen et meget bedre overblik over hele kommunens samlede status på efterlevelsen af GDPR
- en stærkere og tydeligere organisering af den støtte, der er behov for decentralt på dette område

De primære fokusområder i 2022 blev:

- Implementering af system til understøttelse af opgaver på området.
- Styrke organiseringen omkring den støtte, som fagområderne har behov for.
- Deltagelse i Det Fælleskommunale Databehandlersekretariat.
- Implementering af GDPR awarenes i forbindelse med onboarding af nye ledere i Nordfyns Kommune.

De primære fokusområder for 2023 er:

- Fortsat udrulning af systemet Wired Relations til fagområderne.
- Fortsat fokus på at sikre den rette organisering omkring opgavevaretagelsen forbundet med GDPR og informationssikkerhed.
- Udarbejdelse af generelle arbejdsgange og procedurer til organisationen på informationssikkerhedsområdet (harmonisering).
- Udvikling af awarenes til organisationen med henblik på at sikre et passende vidensniveau generelt .

Øvrige bemærkninger:

Det følger af persondataforordningens artikel 38, stk. 3, at DPO'en rapporterer direkte til det øverste ledelses niveau i kommunen. I Nordfyns Kommune er det besluttet, at denne afrapportering (årsberetning) skal ske en gang om året. Årsberetningen er alene til orientering, da der af persondataforordningens artikel 38, stk. 3 tillige fremgår, at databeskyttelsesrådgiveren ikke må modtage instruks i varetagelsen af sit hverv.

Økonomiske oplysninger

Er ikke forelagt Økonomi og Løn

Lovgrundlag

Persondataforordningen

Beslutning

Orientering foretaget.

Bilag

DPO årsberetning 2022