REFERAT Informationssikkerhedsudvalget d. 11-04-2023

Mødedato	Tirsdag d. 11. april 2023 kl. 13:00
Mødested	Bogense Rådhus
Mødedeltagere	Tina Wrøbel, Birgit Mia Larsson, Per Stenaa, Gitte Clemmensen, Vicki Møberg Torp

Indholdsfortegnelse

Punkt 1: Tidsplan

S2021-739

Sagens kerne

Tidsplan

Kl. 13:00 - 13:05	Godkendelse af tidsplan
Kl. 13:05 - 13:20	Risikovurdering - brug af kommunale enheder
Kl. 13:20 - 13:35	Anbefaling til opbevaring af billedmateriale
Kl. 13:35 - 13:45	Implementering af beredskabsplan i praksis
Kl. 13:45 - 13:50	Tilsyn med udpegelse af og rolle for DPO
Kl. 13:50 - 13:55	Redegørelse for håndtering af sagen om brug af Tik Tok
K. 13:55 - 14:00	Årshjul for Informationssikkerhedsudvalget

Beslutning på Informationssikkerhedsudvalget 11-04-2023

Godkendt.

Punkt 2: Risikovurdering - brug af kommunale enheder

S2021-4191

Sagens baggrund

Informationssikkerhedsudvalget har drøftet brug af kommunale enheder på flere møder, senest i februar 2023, hvor det blev besluttet, at den eksisterende brug skulle risikovurderes med henblik på stillingtagen i forhold til eventuelle mitigeringer af risici forbundet hermed.

It-arkitekten fremlægger resultatet af risikovurderingen for informationssikkerhedsudvalget.

Følgende risici er de største = røde lamper:

- Anvendelse af private Apple-id giver risiko for sikkerhedskopiering også af arbejdsrelaterede oplysninger. Brug af Siri gemmer data uden for brugerens kontrol.
- Private apps kan hente oplysninger fra lokale tjenester fra telefonen, herunder fx kamera eller funktionen noter mm. (jf. TikTok-sagen).
- Fælles arbejds- og privat adressekartotek giver en øget risiko for at sende mails forkert.
- Privat Apple-ID kan låse telefonen, så den ikke længere kan bruges ved fratrædelse, med mindre den opsagte medarbejder låser den op ved aflevering.
- Private telefoner deles til tider med familiemedlemmer, herunder børn. Denne brug skaber en øget risiko, som medarbejdere ikke altid er bevidste om eller kan se.
- Login med privat Apple-Id kan potentielt synkronisere data til enheder uden for MDM - lokale kopier uden for kommunens kontrol.
- Bruger kan hente App's til tjenestebrug, som vi ikke ved de anvender.

Der ud over er der 2 risici af mindre betydning, som må forventes at blive håndteret sammen med eventuelle mitigeringer, som udvalget måtte beslutte skal iværksættes. Risikomatricen er vedlagt punktet (faneblad 3).

Informationssikkerhedsteamet anbefaler, at den tekniske sikkerhed på kommunale enheder mitigeres, således at privat brug heraf ikke længere udgør en risiko. Anbefalingen er alene baseret op det forhold, at der ér løsninger tilstede hos andre leverandører, som teknisk vil kunne fjerne risikoen for sammenblanding af private og arbejdsmæssige oplysninger .

Indstilling

Informationssikkerhedsteamet indstiller, at Informationssikkerhedsudvalget beslutter, om de beskrevne risici giver anledning til mitigering, eller om risici kan accepteres ud fra en vurdering af sandsynlighed og konsekvens sat over for de fordele, som den nuværende brug repræsenterer.

Lovgrundlag

Persondataforordningen

Økonomiske oplysninger

Ikke relevant

Sagens kerne

Den eksisterende brug af kommunale enheder er risikovurderet med henblik på stillingtagen til eventuelle ændringer heraf.

Beslutning på Informationssikkerhedsudvalget 11-04-2023

Drøftet.

Informationssikkerhedsudvalget besluttede at mitigere udvalgte risici jf. visualisering b i bilaget, med henblik på fortsat at tillade privat brug af kommunale mobilenheder. Det betyder at en del af de i bilaget beskrevne risici accepteres, selv om den organisatoriske risiko stadig vil være relativt høj efter mitigeringen.

Accept af de resterende risici forudsætter, at udviklingen omkring trusler følges tæt, samt at ændringer i trusselsbillede forelægges Informationssikkerhedsudvalget med henblik på beslutning om eventuelle yderligere mitigeringer. Der ud over forudsætter accepten, at der udarbejdes supplerende informationsmateriale om korrekt brug til alle brugere af kommunale mobile enheder med henblik på at reducere risikoen for sikkerhedsbrud på grund af menneskelige fejl.

Informationssikkerhedsteamet har opgaven sammen med kommunikationskolleger. Informationssikkerhedsudvalget er opmærksomme på, at menneskelige fejl er en konstant sikkerhedsrisiko, som forudsætter en højere grad af tekniske sikkerhedsforanstaltninger, men Informationssikkerhedsudvalget vurderer, at den accepterede risiko efter de valgte mitigeringer opvejes af de organisatoriske fordele, som den fortsatte brug af mobile enheder til privat brug tilvejebringer. Informationssikkerhedsudvalget har tillige lagt vægt på, at privat brug af kommunale enheder giver gensidig fleksibilitet, opleves som et personalegode og indebærer miljøhensyn.

DPO har anbefalet en så sikker teknisk opsætning af mobilenhederne som muligt, hvis privat brug fortsat skal anbefales. Der ud over har DPO orienteret om de yderligere krav der følger af at acceptere en høj risiko, jf. persondataforordningens artikel 35 og 36, som vedrør konsekvensanalyse og evt. inddragelse af Datatilsynet.

Informationssikkerhedsudvalget har taget anbefalingen til efterretning, og tilføjer at mobile enheder ikke har til formål at behandle personoplysninger. Behandling af personoplysninger skal ske i de dertil indrettede ESDH-/fagsystemer. Mitigeringerne vil have fokus på at sikre korrekt brug af mobile enheder.

Bilag

Risikovurdering for personlige apple enheder

Punkt 3: Anbefalinger til opbevaring af billedmateriale

S2023-4950

Lovgrundlag

Persondataforordningen

Sagens baggrund

Nordfyns Kommune har hidtil haft kontrakt med to leverandører af systemer til opbevaring af billeder og film, Dreambroker og Skyfish. Fremadrettet skal vi kun have en leverandører, og valget er faldet på Skyfish, da det er billigst, samt at Skyfish i overordnede træk kan det samme og har samme sikkerhedsmæssige profil som Dreambroker.

I forbindelse med overvejelserne om valg af leverandør er DPO inddraget med henblik på at kvalificere persondatasikkerheden omkring fremadrettet brug af systemet. DPO rådgiver om, at systemet bør have en høj sikkerhedsgrad, idet systemet forventes at skulle opbevare film og lydfiler af børn med særlige udfordringer. Systemet skal også bruges til opbevaring af offentliggjort billedmateriale.

Både Skyfish og Dreambroker er cloudbaserede systemer. Det betyder i praksis, at disse systemer er omfattet af samme uforløste databeskyttelsesudfordringer som Chromebook og andre cloudbaserede systemer, som kommunen allerede har kontrakter med. Samtidig hermed må kommunen forholde sig til, at der ikke umiddelbart eksisterer leverandører på markedet, som kan løfte kommunens behov, uden at data gemmes i cloud.

Kommunens behov for behandling af fortrolige oplysninger i Skyfish udspringer fra Børn og Unge. Sagsbehandlerne kan løse deres kerneopgave i forhold til børn og unge med særlige udfordringer hurtigere og med højere kvalitet ved brug af korte film af børnene, som har til formål at blive udvekslet med forældrene samt at dokumentere barnets udvikling. Dette behov er et af flere væsentlige elementer, som skal indgå i overvejelsen af løsningsmodel. Det bemærkes i denne forbindelse, at der kun gives adgang til de medarbejdere, som her behov for at bruge skyfish til løsningen af deres opgaver. Adgange registreres og holdes opdateret via IDM.

Et andet element er alternative løsningsmodeller til en cloudbaseret leverandør. Så vidt vides eksisterer der på nuværende tidspunkt ikke alternative digitale tjenester, som ikke ligger i cloud og som kan løfte kommunens behov. Det betyder i praksis, at det eneste alternativ til Skyfish eller en lignende leverandør, er en lokal server. Denne model betyder mere bøvlede arbejdsgange for medarbejderne og potentielt samme eller højere omkostninger, uden at sikkerheden bliver højere. Risiciene vil have et andet udtryk, men vurderingen fra It-arkitekten er, at sikkerheden ikke bliver bedre med denne model.

Ud over ovenstående kan Informationssikkerhedsudvalget også tage i betragtning, at kommunen allerede har andre systemer med tilknytning til Cloud. Chromebook-sagen medvirker til, at vi i kommunen bliver bedre rustet til at håndtere systemer, som har dette vilkår med sig, og kommunen vil skulle anvende samme viden og opfølgning på dette system, som på de andre systemer vi har med adgang til skyen. Der er således som udgangspunkt tale om samme risikoprofil for Skyfish som ved andre leverandører kommunen anvender og er bundet til. Nu er Kommunen blot bevidst om det, og kan derfor håndtere vilkåret bedre end tidligere.

Indstilling

Informationssikkerhedsteamet indstiller, at Informationssikkerhedsudvalget træffer beslutning om:

1. at Skyfish skal anvendes til alle typer af billeder og film, herunder også med følsomt indhold eller
2. at Skyfish kun anvendes til billeder og film, som bliver offentliggjort.

Økonomiske oplysninger

Ikke relevant

Sagens kerne

Nordfyns Kommune skal fremadrettet anvende Skyfish til opbevaring af billeder og film. Informationssikkerhedsudvalget skal beslutte, om Skyfish kan anvendes til alle typer film og billeder, eller om systemet kun skal opbevare billeder og film, som er beregnet til offentliggørelse.

Beslutning på Informationssikkerhedsudvalget 11-04-2023

Drøftet.

Indstilling 1 godkendes.
Skyfish risikovurderes og mitigeres efter behov. Erfaringer fra AULA, som også ligger i Amazon Cloud anvendes til risikovurdering af Skyfish. Informationssikkerhedsteamet sikrer dette. Informationssikkerhedsteamet følger trusselsniveauet for Amazon Cloud løbende og orienterer Informationssikkerhedsudvalget herom efter behov.

DPO's bemærkninger om, at brugen af Skyfish (grundet Amazon Cloud) stadig vil udgøre en selvstændig risiko, som kommunen ikke kan mitigere på egen hånd, er taget til efterretning i forbindelse med beslutningen.

Informationssikkerhedsudvalget træffer beslutningen i erkendelse af, at der endnu ikke eksisterer tidssvarende alternativer til løsningen af de behov, som kommunen har i henhold til kerneopgaven.

Punkt 4: Implementering af Beredskabsplan for IT og Informationssikkerhed i Nordfyns Kommune

S2023-1275

Lovgrundlag

Gældende sikkerhedsforskrifter

Sagens kerne

Beredskabsplanen for IT og informationssikkerhed i Nordfyns Kommune skal implementeres. Informationssikkerhedsudvalget skal drøfte, hvordan denne implementering skal ske.

Økonomiske oplysninger

Ikke relevant.

Indstilling

Informationssikkerhedsudvalget drøfter, hvordan Implementeringen af Beredskabsplan for IT og informationssikkerhed skal ske i praksis.

Sagens baggrund

I februar 2023 godkendte Informationssikkerhedsudvalget Beredskabsplanen for IT og Informationssikkerhed i Nordfyns Kommune. Næste skridt er at få beredskabsplanen implementeret i organisationen.

Informationssikkerhedsteamet drøfter hvordan implementeringen skal ske i praksis.

Beslutning på Informationssikkerhedsudvalget 11-04-2023

Drøftet.

Det er besluttet, at den organisatoriske implementering af IT beredskabsplanen skal følge IDM implementeringen samt handleplan for IT- og digitaliseringsstrategien for 2023-2025. Derudover skal der følges op med henblik på at sikre, at beredskabsplanen kommer til at leve i organisationen centralt som decentralt. Informationssikkerhedsteamet sikrer denne opfølgning og rapporterer til Informationssikkerhedsudvalget.

Der ud over skal IT beredskabsplanen knyttes til beredskabsplanen på det tekniske område samt beredskabsplanen på sundhedsområdet. Relevante bidrag fra disse beredskabsplaner indarbejdes i IT beredskabsplanen.

Punkt 5: Tilsyn med udpegelse af og rolle for DPO

S2023-4459

Økonomiske oplysninger

Ikke relevant.

Indstilling

Administrationen indstiller, at Informationssikkerhedsudvalget tager orienteringen til efterretning.

Lovgrundlag

Databeskyttelsesforordningen.

Sagens baggrund

Den 21. marts udsendte datatilsynet en skrivelse vedrørende et skriftligt tilsyn om kommunens udpegning af databeskyttelsesrådgiver og dennes rolle i kommunen. Det skriftlige tilsyn er besvaret i samarbejde mellem DPO og formanden for Informationssikkerhedsudvalget.

Formålet med tilsynet er, at skabe et overblik over databeskyttelsesrådgiverens arbejde og eventuelle udfordringer forbundet hermed. Resultatet af tilsynet bliver samlet i en rapport, som danner grundlag for, om der er behov for mere vejledning af kommunerne i forhold til brugen af databeskyttelsesrådgiverfunktionen.

Det kan ikke udelukkes, at svarene fra det skriftlige tilsyn kan udløse et specifikt tilsyn, men vurderingen er umiddelbart, at Nordfyns Kommune har svaret tilfredsstillingen på de fremsendte spørgsmål. Er denne vurdering korrekt, vil Nordfyns Kommune ikke høre mere fra dette skriftlige tilsyn.

Sagens kerne

Datatilsynet har udsendt link til besvarelse af spørgsmål om udpegning og rolle for DPO.

Beslutning på Informationssikkerhedsudvalget 11-04-2023

Orientering foretaget.

Bilag

Brev fra Datatilsynet (D575907)

Punkt 6: Redegørelse for håndtering af sagen om brug af Tik Tok

S2023-3661

Sagens kerne

Informationssikkerhedsudvalget orienteres om Redegørelse for håndtering af sagen om brug af Tik Tok.

Indstilling

Informationssikkerhedsteamet indstiller, at Informationssikkerhedsudvalget tager orienteringen til efterretning.

Økonomiske oplysninger

Ingen

Lovgrundlag

Persondataforordningen og god skik i den offentlige forvaltning.

Sagens baggrund

På det ekstraordinære informationssikkerhedsudvalgsmøde den 10. marts 2023 blev det besluttet, at der skulle udarbejdes et notat om Nordfyns Kommunes håndtering af Tik Tok sagen.

Notatet forelægges hermed til orientering.

Beslutning på Informationssikkerhedsudvalget 11-04-2023

Orientering foretaget.
IT foretager en sidste indsats i forhold til de resterende brugere, som har Tik Tok installeret på deres mobilenhed, denne gang via brugerens leder/chef.

Bilag

Redegørelse for håndtering af sag om brug af Tik Tok

Punkt 7: Årshjul for Informationssikkerhedsudvalget

S2023-4209

Lovgrundlag

Persondataforordningen.

Økonomiske oplysninger

Ikke relevant.

Indstilling

Informationssikkerhedsudvalget kvalificerer og godkender Årshjul for Informationssikkerhedsudvalget.

Sagens kerne

Årshjulet skal kvalificeres og godkendes af Informationssikkerhedsudvalget

Sagens baggrund

Informationssikkerhedsudvalget har en del faste opgaver, som nu er skematiseret i et årshjul.

Årshjulet skal løbende kvalificeres og tilpasses udviklingen på området, hvorfor årshjulet fremadrettet vil være et fast orienteringspunkt på Informationssikkerhedsudvalgets dagsorden.

Beslutning på Informationssikkerhedsudvalget 11-04-2023

Følgende tilskrives årshjulet:

- Opfølgning og revision af IT Beredskabsplan i 1. kvartal
- IT - revision i 4. kvartal

Årshjulet kvalificeres løbende af Informationssikkerhedsudvalget.

Bilag

Årshjul for Informstionssikkerhedsudvalget