INDENRIGS- OG SUNDHEDSMINISTERIET

Slotsholmsgade 10-12
DK-1216 København K

T +45 7226 9000
F +45 7226 9001
M sum@sum.dk
W sum.dk

Dato: 01-07-2024
Enhed: ISDB-enheden
Sagsbeh.: SAK/ABKN
Sagsnr.: 2024-3855
Akt-id.: 194635

Udvalg for Cyber-, og informationssikkerhed og databeskyttelse (CID-udvalg)

Referat

Tekst fra dagsordenen er medtaget under hvert punkt og er markeret med gråt.

Dato for møde
23. maj 2024

Deltagere

Medlemmer

Cecilie Louise Svane Olesen (CLSO), afd. Strukturel Sundhed, forperson

Trine Brøbecher (TRBR), HR

Carsten Grage (CG), IT

Annette Baun Knudsen (ABKN), ISDB-enheden

Observatører

Helle Ginnerup-Nielsen (HGN), DPO DEP

Philip Joen Bujnoch (PBU), DPO Benchmarkingenheden

Ressourceperson

Frederik Kastoft-Davidsen (FKD), ISDB-enheden

Sekretariat

Sanae Karroum (SAK), ISDB-enheden (referent)

Bilag: For at skabe en bedre sammenhæng mellem dagsorden og bilag, følger bilagene det nummererede punkt på dagsordenen, således at punkt 3's bilag hedder henholdsvis bilag 3.1 og bilag 3.2.

Dagsorden

1. Velkomst
2. Referat fra CID-udvalgsmøde den 29-02-2024
3. Ny sammensætning af CID-udvalg
4. Obligatoriske e-learningskurser
5. Retningslinjer for informationssikkerhed i Indenrigs- og Sundhedsministeriets departement
6. Risikostyring i Indenrigs- og Sundhedsministeriets departement
7. Vurdering af FM's tilsyn med SIT
8. Orientering
    a. ISO-modenhedsmåling og tekniske minimumskrav i Indenrigs- og Sundhedsministeriet
    b. Møde i CID-koordinationsforum 30-04-2024
    c. Handleplan for 2024
    d. Brud på persondatasikkerheden
    e. Oplysningstekst for medarbejdere i ISM
    f. Stikprøvekontrol i F2
    g. Status på retningslinjer for indberetning af sikkerhedshændelser
    h. Status vedr. implementering af fuld decentral koncern it-model
9. Eventuelt
10. Næste møde

Dagsorden

1. Velkomst

CLSO bød velkommen til udvalgets andet møde og spurgte, om udvalget havde bemærkninger til dagsordenen. Udvalget havde ingen bemærkninger.

2. Godkendelse af referat fra CID-udvalgsmøde den 29-02-2024

Indstilling

. / . Det indstilles, at CID-udvalget godkender referat fra CID-udvalgsmøde den 29-02-2024 (bilag 2.1).

Sagsfremstilling:
Referat fra CID-udvalgets møde den 29-02-2024 er udsendt til udvalgets medlemmer den 03-04-2024. Der er ikke modtaget bemærkninger til referatet.

Den videre proces
Med udvalgets godkendelse vil referatet blive offentliggjort på ISM INTRA.

Bilag
2.1. Referat fra CID-udvalgsmøde 29-02-2024.

Beslutning
Udvalget godkendte referatet uden yderligere bemærkninger.

3. Ny sammensætning af CID-udvalg

Indstilling

. / . Det indstilles, at CID-udvalget godkender den nye sammensætning af udvalget (bilag 3.1 og 3.2).

Sagsfremstilling:
Den 1. marts 2024 blev der implementeret en organisationsændring i Indenrigs- og Sundhedsministeriet med det formål at tilpasse organisationens struktur og prioritere de opgaver, som departementet står overfor.

Som følge af organisationsændringen er det nødvendigt at foretage en gennemgang af CID-udvalgets medlemmer for at sikre en rigtig koordinering på tværs af organisationen.

. / . ISDB-enheden har udarbejdet et forslag til den nye sammensætning, jf. bilag 3.1 og bilag 3.2. De væsentligste ændringer i forslaget er, at afdelingschef Dorthe Bech Vizard udtræder som medlem af udvalget, og at sektionsleder Pernille Seaton fremover er tilknyttet som ressourceperson.

Bilag
3.1. Medlemmer af Cyber-, Informationssikkerhed og Databeskyttelsesudvalget.

3.2. Kommissorium for CID-udvalg

CLSO indledte og præsenterede udkastet til den nye sammensætning for CID-udvalget.

CLSO bemærkede, at de væsentligste ændringer er, at Dorthe Vizard er udtrådt af udvalget, og at Pernille Seaton er tilknyttet som ressourceperson.

Beslutning
Udvalget godkendte den nye sammensætning af CID-udvalget.

4. Obligatoriske e-learningskurser

Indstilling

./. Det indstilles, at CID-udvalget godkender, at kurset "Cyber- og informationssikkerhed for topledere og ledere i staten" føjes til listen over obligatoriske kurser (bilag 4.1), og at ISDB-enheden trækker lister på, hvem der har og ikke har gennemført kurserne.

Der lægges endvidere op til en drøftelse af om kurserne skal tages en gang under ansættelsen eller en gang årligt.

Sagsfremstilling
På nuværende tidspunkt er følgende campus-kurser obligatoriske for medarbejdere: "Cyber- og informationssikkerhed for medarbejdere" og "Databeskyttelse"

På det seneste udvalgsmøde blev det besluttet, at ISDB-enheden skulle undersøge eksisterende obligatoriske kurser inden for CID-området og vurdere behovet for eventuelle tilføjelser til listen over obligatoriske kurser. Efter en gennemgang har ISDB-enheden vurderet, at kurset Cyber- og informationssikkerhed for topledere og ledere i staten bør tilføjes som obligatorisk kursus.

Dette kursus er blevet vurderet som relevant for topledere og ledere, da det giver en introduktion til grundlæggende begreber inden for cyber- og informationssikkerhed samt til ledelsens ansvar og opgaver på dette område.

ISDB-enheden foreslår, at enheden udarbejder årlige lister over hvem, der har og ikke har gennemført de obligatoriske kurser med henblik på en overordnet drøftelse af listerne i CID-udvalget den 13. november 2024. Cheferne for de medarbejdere der ikke har gennemført kurserne vil ligeledes blive informeret mhp., at de kan påminde deres medarbejdere om at gennemføre kurserne inden udgangen af året.

Den videre proces
ISDB-enheden kontakter HR mhp. at kurset tilføjes listen over obligatoriske kurser. ISDB-enheden vil fremadrettet en gang årligt trække lister på, hvem der har og ikke har gennemført kurset og orientere om det på et CID-udvalgsmøde.

Bilag
4.1 Overblik over nuværende obligatoriske kurser

CLSO indledte med at bemærke, at CID-udvalget på sidste møde (29-02-2024) blev enige om, at ISDB-enheden skulle udarbejde et forslag til, hvilke informationssikkerheds- og databeskyttelsesretlige kurser, der skulle gøres obligatoriske i ISM.

CLSO gav herefter ordet til ABKN, som redegjorde for ISDB-enhedens forslag som beskrevet i sagsfremstillingen om, at de to obligatoriske kurser indenfor Informationssikkerhed og databeskyttelse: "Cyber- og informationssikkerhed for medarbejdere i staten" og "Databeskyttelse" forbliver obligatoriske, og at kurset "Cyber- og Informationssikkerhed for topledere og ledere i staten" føjes til listen over obligatoriske kurser for ledere i departementet.

Der var herefter en drøftelse af, om ledere skal tage både Cyber- og informationssikkerhed for medarbejdere i staten og kurset "Cyber- og Informationssikkerhed for topledere og ledere i staten, samt en drøftelse af, hvor ofte kurserne skal tages, én gang årligt eller en gang under ansættelsen.

ABKN orienterede om, at ISDB-enheden vil forsøge at få plads på chefmødet den 12. juni 2024 til at kommunikere om kurser, retningslinjer for informationssikkerhed, jf. punkt 5, og retningslinjer for indberetning af sikkerhedshændelser.

Beslutning:
Udvalget godkendte i overensstemmelse med indstillingen,
At kurset "Cyber- og informationssikkerhed for topledere og ledere i staten" føjes til listen over obligatoriske kurser, og at alle ledere i departementet skal tage kurset.

At de nuværende campus-kurser " Cyber- og informationssikkerhed for medarbejdere i staten" og "Databeskyttelse" forbliver obligatoriske for alle medarbejdere i departementet.

At ISDB-enheden en gang årligt (i efteråret) trækker en liste over, hvem der har/ ikke har gennemført kurserne det seneste år med henblik på at listerne kan forelægges CID-udvalget listerne på mødet i november måned. CID-udvalget besluttede desuden, at denne status for gennemførsel af kurser skulle forelægges chefgruppen for så vidt angår medarbejdere og AC-gruppen for så vidt angår chefer.

Udvalget besluttede endvidere, at ISDB-enheden undersøger, om det er relevant for ledere at tage begge kurser og forelægger dette for udvalget på ny.

Det bemærkes, at ISDB-enheden efter mødet har taget kurserne, og der er ikke overlap. CID-udvalget har efterfølgende i skriftlig proces, jf. ISDB-enhedens mail af 6. juni 2024 til CID-udvalget, godkendt at kurserne Cyber- og informationssikkerhed for medarbejdere i staten" og "Databeskyttelse" skal forblive obligatoriske for alle medarbejdere i departementet, inkl. ledere, og at ledere herudover også skal tage kurset "Cyber- og informationssikkerhed for topledere og ledere i staten.

5. Retningslinjer for informationssikkerhed i Indenrigs- og Sundhedsministeriets departement

Indstilling

./. Det indstilles, at CID-udvalget drøfter og godkender retningslinjer for informationssikkerhed målrettet medarbejdere i Indenrigs- og Sundhedsministeriet (bilag 5.1).

Sagsfremstilling

IT-sikkerhedsstandarden ISO27001 indebærer, at statslige institutioner skal etablere et ledelsessystem for informationssikkerhed (ISMS), hvorefter der fastsættes politikker, procedurer og retningslinjer for informationssikkerhed for den enkelte institution.

Retningslinjer for medarbejdere i Indenrigs- og Sundhedsministeriet fastsætter regler for it-anvendelsen og fastlægger en minimumsstandard for it-anvendelsen, men fastlægger også reglerne for adgang til ministeriets bygninger, håndtering af gæster, samt beskriver informationstyper og deres korrekte anvendelse mv.

Selv om retningslinjerne dækker et bredt område, udelukker det ikke, at der også findes eller udarbejdes uddybende procedurer og retningslinjer inden for områderne. F.eks. kan der være supplerende rejsevejledninger, sikker mobilopsætning på sikrede enheder osv., som medarbejderne kan forholde sig til, når det er relevant.

Retningslinjerne bygger i stort omfang på retningslinjer fra indenrigsdelen og vil derfor være genkendelige for en del af medarbejderne. Sundhedsdelen havde sammenlignelige regler, der var udarbejdet af SDS.

ISDB-enheden vil i løbet af 2025 vurdere, om der er behov for at opdatere retningslinjer for informationssikkerhed og forelægge eventuelle ændringsforslag for CID-udvalget.

Den videre proces
Med udvalgets godkendelse vil retningslinjerne (inkl. evt. justeringer) blive præsenteret for chefkredsen på et chefmøde.

Retningslinjerne (inkl. evt. justeringer) vil herefter blive behandlet i Samarbejdsudvalget, hvorefter de er endeligt godkendt.

Retningslinjerne vil i forlængelse heraf blive formidlet til medarbejderne på ISM INTRA, hvorefter kontorcheferne orienterer medarbejderne på kontormøderne.

ISDB-enheden vil desuden i samarbejde med kommunikation udarbejde informationsmateriale om retningslinjerne, herunder kortere udgaver af retningslinjerne mv.

Retningslinjerne vil endvidere indgå i on-boarding forløbet for nyansatte.

Bilag
5.1 Retningslinjer for informationssikkerhed

CLSO indledte med at bemærke, at dette punkt er både til drøftelse og godkendelse.

CLSO præsenterede punktet, hvorefter ordet blev givet til ABKN.
ABKN oplyste, at PBJ har udarbejdet udkastet med udgangspunkt i IM's tidligere retningslinjer. ISDB-enheden har herudover forud for mødet drøftet retningslinjerne med HR, HGN, og for så vidt angår afsnit 4.2 med Katja Roitmann, hvilket har ført til en række tilpasninger.

ABKN bemærkede, at manglende overholdelse af retningslinjerne vil kunne føre til ansættelsesretlige reaktioner, og at retningslinjerne derfor også skal behandles af Samarbejdsudvalget, jf. forslag til videre proces. ABKN bemærkede, at planen er, at retningslinjerne kommer på Samarbejdsudvalget den 25. juni 2024.

ABKN orienterede desuden om, at Justitsministeriet kort før mødet (den 16. maj) har udgivet opdaterede retningslinjer for statslige myndigheders opbevaring af SMS-beskeder m.v. Disse retningslinjer er sammenholdt med retningslinjerne for Informationssikkerhed, og der vurderes ikke at være uoverensstemmelser. Justitsministeriets retningslinjer blev omdelt på mødet.

Udvalget drøftede herefter retningslinjerne.

HGN oplyste, at hun forud for udvalgsmødet har afgivet en række bemærkninger, og at retningslinjerne er blevet tilpasset i forhold til flere af disse bemærkninger. HGN understregede, at der sagtens kan være gode og legitime grunde til, at ikke alle bemærkninger, hvoraf en del blot havde karakter af opmærksomhedspunkter, var imødekommet i det foreliggende udkast.

HGN gjorde dog opmærksom på, at hun fortsat finder, at følgende sætning i punkt 8 "Lokal- og fællesdrev": *"Krypteret data kan lagres på fildrevene uanset deres indhold, under forudsætning af, at dataminimeringsprincippet opretholdes, og at der er et arbejdsbetinget formål med lagringen"* bør genovervejes med henblik på enten at udgå, omformuleres eller suppleres, så det sikres, at retningslinjerne er i overensstemmelse med databeskyttelsesretlige krav. HGN bemærkede, at det i den forbindelse ikke er tilstrækkeligt at henvise til dataminimeringsprincippet.

Det blev drøftet, om sætningen var nødvendig for medarbejderne eller eventuelt kunne udgå. CG bemærkede, at det er nødvendigt med denne sætning, idet der i CPR-kontoret er behov for, at medarbejdere kan arbejde på fildrev fx i Excel ark, som indeholder krypterede personoplysninger.

CSO bemærkede, at rækkefølgen på de sidste to afsnit bør ændres, således at pointen med, at der skal ryddes op løbende kommer til at gælde også for krypterede data.

Beslutning

Udvalget godkendte retningslinjerne for informationssikkerhed målrettet medarbejdere i Indenrigs- og Sundhedsministeriet, dog således at punkt 8 Lokal- og fællesdrev skulle justeres i lyset af bemærkninger fremsat på mødet.

Udvalget godkendte den foreslåede videre proces (herunder forelæggelse på chef-møde, Samarbejdsudvalg, kommunikation på intra, udarbejdelse af informationsmateriale i samarbejde med kommunikation, samt at retningslinjerne indgår i on-boarding forløb for nyansatte)

Udvalget godkendte endvidere, at ISDB-enheden genbesøger og forelægger retningslinjerne efter behov og senest i 2025, og at CID-udvalget i den forbindelse tager stilling til fremtidig frekvens for gennemgang af retningslinjerne.

Det bemærkes, at ISDB-enheden efter mødet i CID-udvalget den 23. maj 2024 i samarbejde med IT og under inddragelse af HGN/DPO justeret punkt 8, hvor en række af HGNs bemærkninger og forslag er imødekommet. De endelige retningslinjer er godkendt af CID-udvalget i skriftlig proces. Der henvises i den forbindelse til ISDB-enhedens e-mail af 6. juni 2024 til CID-udvalget, hvori ISDB-enheden også gør opmærksom på, at HGN/DPO har tilkendegivet, at det ikke er alle HGN's betænkeligheder i forhold til departementets efterlevelse af GDPR, der er imødekommet. Herunder er det ikke afdækket, om der foreligger fyldestgørende risikovurdering(er) relateret til behandlingen af personoplysninger på drevene, hvori der er taget stilling til og dokumenteret, hvilke sikkerhedsforanstaltninger der i lyset af bl.a. karakteren af oplysningerne er nødvendige, og om alle nødvendige foranstaltninger er implementeret.

Det fremgår videre af denne mail, at HGN i den forbindelse bl.a. har hæftet sig ved, at der i forbindelse med gennemgangen af retningslinjerne er blevet afdækket et behov for at genbesøge opsætningen af adgangsbegrænsningen på nogle af kontordrevene, så det fremover kun er medarbejdere i de enkelte kontorer, der har adgang. Endvidere har HGN bemærket, at det ikke står helt klart, om behandlingen kan og bør ske i F2 i stedet, om end der for så vidt angår F2 (generelt) også synes at være et presserende behov for at genbesøge relevante risikovurderinger, særligt ift. adgangsstyring. HGN er enig i, at det er vigtigt at få retningslinjer ud til medarbejderne.

6. Risikostyring i Indenrigs- og Sundhedsministeriets departement

Indstilling
Det indstilles, at CID-udvalget drøfter udkast til risikostyringsproces i departementet og godkender udkastets forslag til ramme for:

- Interessentanalyse
- Roller og ansvar
- Risikoprioritering

Det indstilles endvidere, at CID-udvalget godkender forslag til videre proces.

Sagsfremstilling
ISDB-enheden har i bilag 6.1. udarbejdet en præsentation om risikostyring i departementet, som vil blive gennemgået på CID-udvalgsmødet. Præsentationen giver et overblik over de væsentligste drøftelsespunkter og projektplanen. Det samlede udkast til risikostyringsproces er vedlagt som bilag 6.2.

Risikostyringsprocessen er udviklet på baggrund af principperne i ISO 27005:2018 og Digitaliseringsstyrelsens vejledning i risikostyring. Processen er yderligere forankret i ledelsessystemet jf. CID-politikken og CID-udvalgets kommissoriums roller, ansvar og målsætninger.

Processen definerer: 1) typer af informationsaktiver der er underlagt risikovurdering (systemer og processer), 2) typer af risikovurderinger der skal udføres (sikkerhedsrisici), 3) metodik for ensartet risikostyring, 4) roller og ansvar ifm. risikovurdering og risikohåndtering (risikoejere, som typisk vil være kontorchefer, ISDB-enheden, DPO, CID-udvalget, topledelse), 5) rapportering og eskalering af risiko ifm. risikohåndtering.

ISDB-enheden vurderer, at implementering af risikostyring vil forudsætte et ressourceforbrug blandt risikoejere, CID-udvalget og ISDB-enheden. Ressourceforbruget vil aftage efter implementering, men afhænge af graden af kommunikation og træning, systemunderstøttelse, samt kompetencer og erfaring hos de relevante rolleindehavere i processen.

Det skal bemærkes, at udkastet til risikostyringsproces indeholder en række forslag vedr. den bredere arkitektur iht. departementets ledelsessystem som vedrører interessentanalyse og risikoappetit, roller og ansvar, samt risikoprioritering. Da disse forslag vurderes at være en forudsætning for en effektiv og operationel implementering af processen, anbefales det, at CID-udvalget tager stilling til og vurderer indholdet i disse forslag.

Det bemærkes endvidere, at udkastet til risikostyringsproces (bilag 6.2) indeholder en række afsnit, der skal afstemmes med CID-udvalget og andre dele af departementet. I

bilaget er kommentarer bibeholdt mhp. at øge læsevenligheden og fremhæve de afsnit, hvor ISDB-enheden vurderer, at afstemning er nødvendig.

Den videre proces
ISDB-enheden vil med udvalgets godkendelse, inkl. de justeringer der evt. besluttes på mødet, arbejde videre med risikostyringsprojektet. Som en del af projektet vil ISDB-enheden indsamle bidrag fra CID-udvalget og øvrige afdelinger i departementet ift. at gøre processen klar til implementering. Den færdige risikostyringsproces vil blive forelagt på næste CID-udvalgsmøde i september, jf. projektplan side 7 i bilag 6.1.

Bilag
6.1 Præsentation – drøftelsespunkter, projektplan og videre proces
6.2 Risikostyringsproces

CLSO indledte med at bemærke, at dette punkt, som det fremgår af indstillingen, er til drøftelse for så vidt angår det samlede udkast til risikostyringsproces og til godkendelse for så vidt angår den foreslåede videre proces, og de foreslåede rammer for risikostyringsprocessen, jf. indstilling.

CLSO gav herefter ordet til FKD, der præsenterede ISDB-enhedens foreløbige arbejde med risikostyring i departementet.

Udvalget drøftede herefter udkastet til risikostyringsproces i departementet. Bemærkningerne gengives kort her:

- CG bemærkede, at en del områder i den tidligere indenrigsdel havde en måde at arbejde med risikostyring på, og at der er ønske om dels at kunne genbruge eksisterende risikovurderinger, dels at kunne videreføre eksisterende metoder for udarbejdelse af risikovurderinger
- FKD bemærkede, at formålet med risikostyringen er, at der skabes en ensartet tilgang i hele departementet.
- CLSO bemærkede hertil, at der var områder i det tidligere Sundhedsministeriem, hvor man ikke tidligere havde arbejdet med risikostyring, og som derfor skulle starte fra bunden.
- CG bemærkede endvidere, at det ikke er alt, der skal risikovurderes i departementet. Hvis det er forretningskritisk, skal det risikovurderes.
- HGN og FKD bemærkede, at alle behandlingsaktiviteter, hvori der indgår personoplysninger, som udgangspunkt skal vurderes i relation til risici for registrerede/fysiske personer.
- Udvalget drøftede herefter, hvad ISDB-enheden har behov for for at kunne komme videre med arbejdet. FKD oplyste, at ISDB-enheden har behov for at lave en interessentanalyse af hele departementet for at afdække området, herunder afdække roller og ansvar, hvem der godkender hvad mv., samt at det er nødvendigt, at alle kontorer bidrager hertil
- HGN spurgte ind til interessentanalysen, herunder om den også omfattede overholdelse af alle relevante lovkrav. FKD bekræftede dette og henviste til, at risikostyringsprocessen også vedrører ISO 27701, som vedrører overholdelse af databeskyttelsesretlige krav.
- CLSO bemærkede, at det skulle undersøges, om allerede gennemførte risikoanalyser i et eller andet omfang kan genbruges, men at der omvendt også er behov for, at der gennemføres risikoanalyser i hele departementet, og at ledelsen skal have ledelsesrapportering i et format, som gør det muligt at få et overblik.

- CLSO anbefalede, at der blev lagt et ekstraordinært CID-udvalgsmøde ind før sommerferien for at drøfte det videre arbejde med risikostyring, herunder interessentanalyse.

Konklusion
Det blev besluttet at holde et ekstraordinært CID-udvalgsmøde inden sommerferien i juni måned, hvor punktet kunne drøftes yderligere med udgangspunkt i 2 eksempler: et eksempel som IT er system og/eller procesejer på og et eksempel som KOK/tilskudsteamet er system og/eller procesejer på.

Ved e-mail af 25. juni 2024 til CID-udvalget foreslog ISDB-enheden, at dette møde blev aflyst, idet ISDB-enheden gerne vil sætte arbejdet med risikostyringsproces i bero og i stedet prioritere at få opdateret fortegnelser, hvilket er et andet prioriteret indsatsområde i 2024 (jf. i øvrigt punkt 8c på dagsorden til CID-udvalgsmøde den 23. maj 2024).

ISDB-enheden har i den forbindelse henvist til, at den viden vi får om departementets behandlingsaktiviteter i forbindelse med opdatering af fortegnelserne, som er en bunden opgave, vil kunne bruges hensigtsmæssigt til at definere det forventede ressourceforbrug i forbindelse med risikovurdering af processer og understøttende systemer.

I forhold til det videre arbejde med risikostyringsproces vil dette tage udgangspunkt både i udkast til risikostyringsproces, som blev drøftet på CID-udvalgsmødet den 23. maj 2024 og de eksisterende risikovurderinger, som er udarbejdet, ligesom den viden vi får fra opdatering af fortegnelserne også vil indgå.

ISDB-enheden giver en status på arbejdet med fortegnelser og risikostyringsproces på CID-udvalgsmødet til september.

7. Vurdering af FM's tilsyn med SIT

Indstilling
./. Det indstilles, at CID-udvalget behandler FM's tilsyn med SIT med henblik på at vurdere, om rapporten (bilag 7.1 og 7.2) giver anledning til bemærkninger fra ISM.

Sagsfremstilling
Finansministeriet (FM) fører tilsyn med Statens It (SIT) på vegne af kunderne, idet opgaverne med it-driften er ressortoverdraget til FM.

FM leverer årligt en tilsynsrapport en rapport for it-driften og en rapport for kontroller med databeskyttelsesområdet, der sammenfatter tilsynets aktiviteter og bemærkninger for det foregående år.

SIT's kunder er forpligtet til at forholde sig til tilsynets resultater, bl.a. med henblik på at vurdere, om tilsynet giver anledning til handlinger hos kunden eller til at afgive bemærkninger til KRT (nu CTJ).

Af tilsynsrapporterne for 2023 fremgår det bl.a., at:

”Tilsynet finder generelt, at SIT har eller er i gang med at adressere risiciene på de relevante områder, og at SIT generelt har en god og hensigtsmæssig systematik for opfølgning på bemærkninger fra både tilsynet og Rigsrevisionen”

Samt at:

”Resultaterne af tilsynet med SIT’s rolle som databehandler viser, at SIT overordnet opfylder kravene i GDPR. Tilsynets vurderinger og tests, herunder de individuelle it-tilsynsundersøgelser i fht. GDPR, har dog i enkelte tilfælde afgivet bemærkninger, som kan udgøre en risiko ved behandlingen af data.”

Det fremgår også, at Statens It er certificeret efter ISO-standarderne (bl.a. 20000 og 27001) og ITIL, mv.

Det bemærkes, at ISM-departement er omfattet af standardopsætningen hos SIT, og at driften ikke adskiller sig væsentligt fra SITs andre kunder. Det er derfor typisk tilstrækkelig for ISM, at de anførte forhold udbedres og kontrolleres i henhold til CTJ’s tidsplan.

IT og ISDB-enheden har vurderet materialet og er af den opfattelse, at der ikke er behov for yderligere opfølgning over for CTJ.

Den videre proces
Hvis der er bemærkninger til FM’s tilsyn, sender ISDB-enheden bemærkningerne til CTJ.

Bilag
7.1 Beretning om tilsynet med SIT 2023
7.2 Tilsynsrapport nr. 1 2023 SIT som databehandler

CLSO indledte og gav ordet til ABKN,
ABKN præsenterede punktet, herunder at IT og ISDB-enheden vurderede, at der ikke var behov for yderligere opfølgning over for CTJ (tidligere KTR).

ABKN supplerede med at oplyse, at det bl.a. fremgår af den overordnede konklusion i rapporten ”Tilsyn med SIT som databehandler”, april 2024 (side 4), at der er en høj beskyttelse hhv. effektiv beskyttelse, se rapportens side 4, tabel 1.

Det blev drøftet, at KRT havde en enkelt kritisk tilsynsbemærkning vedr. behandlingssikkerhed, jf. rapportens side 17, hvoraf det bl.a. fremgår, at Tilsynet fandt det særligt kritisk, at 300 medarbejdere havde adgang til kundernes SMS-data, idet der var tale om potentielt følsomme og personlige data for en særlig personkreds. Potentielt ville det ikke give nogen særlig risiko for brud på fortroligheden, idet kunderne skulle levere disse data krypteret. Det fremgår imidlertid, at KRT havde konstateret, at der var mange tilfælde, hvor kunderne ikke havde krypteret deres data. KRT og SIT har foretaget en gennemgang og konstateret, at data ikke var tilgået af personer i SIT, hvorfor der de facto ikke var tale om, at medarbejdere havde fået kendskab til data uden at have et arbejdsmæssigt behov.

CG oplyste, at IT følger op herpå og således er i gang med en intern undersøgelse af, om de SMS’er, som Indenrigs- og Sundhedsministeriet har videregivet til opbevaring hos SIT, har været tilstrækkeligt krypterede.

Beslutning

Udvalget godkendte FM's tilsyn med SIT og fandt ikke, at der er behov for yderligere opfølgning overfor KRT (CTJ).

8. Orientering

8.a ISO-modenhedsmåling og tekniske minimumskrav i Indenrigs- og Sundhedsministeriet

Indstilling
Det indstilles, at CID-udvalget tager orienteringen til efterretning.

Sagsfremstilling
Indenrigs- og Sundhedsministeriets departement skal afrapportere til Digitaliseringsstyrelsen på ISO 27001 modenhedsmåling for 2024 og de tekniske minimumskrav for første halvdel af 2024.

ISO-modenhedsmåling og de tekniske minimumskrav har begge været i høring, og der har ikke været bemærkninger. Indenrigs- og sundhedsministeriets departements måling er sendt til Digitaliseringsstyrelsen.

CPR-kontorets ISO 27001 modenhedsmåling er for 2024 på niveau 5 for alle spørgeområder. Den resterende del af departementet er på modenhedsniveau 4 på 2 af 9 områder i 2024, idet der er sket en forbedring på et enkelt spørgeområde siden 2023

Efterlevelsen af de tekniske minimumskrav er uændret i forhold til seneste afrapportering i august 2023 for både CPR-kontoret og DEP. CPR-kontoret har fortsat et enkelt udestående punkt, som vil blive efterlevet i 2024, mens DEP efterlever de 20 tekniske minimumskrav.

ABKN orienterede om punktet, herunder om, at udvalget har fået sendt udkast til ISO-modenhedsmåling og tekniske minimumskrav i høring inden afrapportering er sendt til Digitaliseringsstyrelsen.

ABKN oplyste videre, at afrapporteringen i år var blevet delt op således, at CPR-enheden er blevet målt adskilt fra resten af departementet. CG bemærkede hertil, at CPR har deres egen organisering ift. CPR-området, hvorfor det har været mest hensigtsmæssigt at udføre målingen på denne måde.

Udvalget tog orienteringen til efterretning.

8.b Møde i CID-koordinationsforum 30-04-2024

Indstilling
Det indstilles, at CID-udvalget tager orienteringen til efterretning.

Sagsfremstilling
CLSO orienterer kort fra mødet.

ABKN indledte med at orientere om, at det væsentligste for CID-udvalget fra CID-koordinationsforumsmødet er afdækning af den fuldstændige decentrale koncern IT-model, som er beskrevet nærmere under punkt 8.d.

PBJ bemærkede, at IT-delen har fremsendt bemærkninger til ISDB-enheden, som skulle sendes videre til SDS. HGN tilføjer hertil, at hun ønsker at få tilsendt en kopi af bemærkningerne til orientering. ABKN oplyser, at ISDB følger op på begge dele.

8.c Handleplan og indsatsområder for 2024, jf. målsætning i CID-politik

Indstilling
Det indstilles, at CID-udvalget godkender, at ISDB-enheden fokuserer på følgende tre indsatsområder i 2024:

- Risikostyring
- Uddannelse og oplysning
- Fortegnelser

Sagsfremstilling
CID-udvalget har i CID-politikken fastlagt følgende målsætninger for departementets arbejde med cyber-, informationssikkerhed og databeskyttelse:

1) Departementets ledelsessystem for cyber-, informationssikkerhed og databeskyttelse er velfungerende og følger kravstandarderne ISO 27001 og ISO 27701, herunder bl.a. ift. løbende godkendelse og vedligehold af:
    a. systemoversigt over departements systemer og processer, herunder departementets artikel 30-fortegnelser.
    b. departementets retningslinjer for arbejdet med risici og trusselskatalog.
    c. departementets SoA (Statement of Applicability), hvor relevante kontroller og foranstaltninger udvælges og vurderes med henvisning til væsentlig dokumentation og gaps.
2) Ledere og medarbejderes viden og bevidsthed om cyber-, informationssikkerhed og databeskyttelse understøttes og øges vha. awareness-tiltag.
3) Der er klarhed om roller, ansvar og opgaver blandt departementets forskellige aktører i CID-arbejdet.
4) Efterlevelse af de tekniske minimumskrav, skærpede krav til kontrakt- og leverandørstyring for kritisk it-infrastruktur og tiltag for styrket cybersikkerhed.
5) Status for den samlede implementering af ISO27001 og ISO 27701 rapporteres til CID-udvalget mindst en gang om året.
6) Status for den samlede implementering af ISO27001 og ISO27701 rapporteres til departementschefen mindst en gang om året.

For at understøtte dette arbejde udarbejder CID-udvalget etårige handleplaner.

ISDB-enheden har identificeret følgende tre områder, der vil blive prioriteret i resten af 2024:

- Risikostyring
- Uddannelse og oplysning
- Fortegnelser

Disse områder er blevet udvalgt med udgangspunkt i ISO27001 og ISO27701. ISDB-enheden arbejder videre på at forelægge CID-udvalget en samlet handleplan som omfatter alle målsætningerne i CID-politikken.

Videre proces
ISDB-enheden fortsætter arbejdet med at implementere de tre fokusområder, samt på at udarbejde en samlet handleplan, som omfatter alle målsætningerne i CID-politikken.

ABKN præsenterede ISDB-enhedens tre fokusområder, jf. sagsfremstillingen (risikostyring, uddannelse og oplysning, samt fortegnelser). ABKN tilføjede, at ISDB-enheden sideløbende vil udarbejde en handleplan og et SoA dokument.

HGN bemærkede, at SoA dokumentet er essentielt for at toplederne i departement har overblik over, hvordan situationen er i departementet på nuværende tidspunkt.

CID-udvalget havde ikke yderligere bemærkninger til indstillingen.

8.d Brud på persondatasikkerheden

Indstilling
Det indstilles, at CID-udvalget tager orienteringen til efterretning.

Sagsfremstilling
I perioden fra 1. januar 2024 til 15. maj 2024 har der været 3 hændelser. To af bruddene vedrørte Nationalt Center for Etik og et brud vedrørte Indenrigs- og Sundhedsministeriets departementet.

- Brud 1) Mistet arbejdscomputer i tog (NCE)
- Brud 2) Fortrolige oplysninger videregivet til Folketinget (ISM)
- Brud 3) Uautoriseret brugeradgang til 3 personer (NCE)

Bilag
8.d.1 Hændelser i 2024

ABKN gav ordet til SAK, der kort gennemgik de tre hændelser, der har været i departementet i 2024.

Udvalget drøftede herefter følgende til punktet:

- PBJ spurgte om departementet har en relation til NCE. SAK oplyste, at departementets DPA ligeledes er DPA for NCE.
- PBJ informerede, at der var en sag på vej til ISDB-enheden, hvor der i første omgang var mistanke om et brud, men efter nærmere undersøgelse, viste det sig, at der ikke var tale om et brud alligevel. Sagen vil blive sendt til orientering.
- HGN bemærkede, at til trods for, at ISDB-enheden udelukkende havde hørt om tre sager, så var der formentlig et langt større mørketal i departementet.
- TRBR tilføjede, at der bør fokuseres mere på awareness for hændelser, således at medarbejderne ved, hvornår de skal indrapportere en hændelse, da mange eksempelvis ikke ved hvad personoplysninger er og hvornår noget er et brud. ABKN oplyste, at det tidligere i CID-udvalget var blevet besluttet at opdatere processen for indberetning af sikkerhedshændelser, og at dette skal præsenteres på et chefmøde, hvorefter det vil blive lagt på intranettet som en nyhed.

Beslutning
Udvalget tog orienteringen til efterretning.

8.e Oplysningstekst for medarbejdere i ISM's departement

Indstilling
Det indstilles, at udvalget tager orienteringen til efterretning.

Sagsfremstilling

Indenrigs- og Sundhedsministeriets departement behandler personoplysninger om departements medarbejdere. Med denne behandling af personoplysninger følger et ansvar, da medarbejderne har en række rettigheder ifølge databeskyttelsesforordningen.

Departementet har ikke tidligere haft en privatlivspolitik for medarbejdere. For at opfylde vores forpligtelse ifølge databeskyttelsesforordningen er ISDB-enheden i færd med at udarbejde en privatlivspolitik for medarbejdere i departementet med input fra relevante enheder og DPO.

Den videre proces
Oplysningsteksten vil blive formidlet til medarbejderne på ISM INTRA og indgå i on-boarding processen til nyansatte.

Bilag
8.e.1 Oplysningstekst for medarbejdere i departementet

CLSO gav ordet til SAK.

SAK indledte med at bemærke, at punktet var på under sidste CID-udvalgsmøde i februar 2024, hvor det blev aftalt, at punktet skulle sendes i skriftlig godkendelse. Da sagen har trukket længere ud end forventet, præsenteres oplysningsteksten til orientering under dagens møde. Oplysningsteksten vil blive formidlet til medarbejderne på INTRA og indgå i on-boarding processen til nyansatte.

Under punktet blev følgende ting drøftet:

- SAK indledte med at bemærke, at punktet alene var til drøftelse, og at det var en fejl, at der i oplysningsteksten fremgik, at punktet var godkendt af CID-udvalget.
- HGN bemærkede, at oplysningsteksten har været længere undervejs, at det er meget positivt, at den kommer ud til medarbejderne, men at det er vigtigt at være opmærksom på behovet for løbende opdatering, f.eks. som følge af opdatering af fortegnelsen over behandlingsaktiviteter.

Beslutning
Udvalget tog orienteringen til efterretning.

8.f Stikprøvekontroller i F2

Indstilling
Det indstilles, at CID-udvalget tager orienteringen til efterretning

Sagsfremstilling
Departementet udfører halvårligt stikprøvekontroller med medarbejdernes anvendelse af F2. Stikprøverne afdækker bl.a., om sagerne er beskyttet med korrekt indblik, og om sagerne tilgås ud fra et arbejdsbetinget behov. Stikprøvekontrollen er udført for perioden indtil april 2024.

Kontrollen har ikke givet anledning til bemærkninger

CLSO gav ordet til CG, der oplyste, at departementet ifølge egne retningslinjer skal udføre stikprøvekontroller to gange om året i F2. Det udføres på den måde, at et antal medarbejdere udvælges, hvorefter det undersøges hvilke sager medarbejderne har tilgået.

Beslutning
Udvalget tog orienteringen til efterretning.

8.g Status vedr. implementering af fuld decentral koncern it-model

Indstilling
Det indstilles, at CID-udvalget tager orienteringen til efterretning.

Sagsfremstilling
På CID-udvalgets møde den 29. februar 2024 blev beslutningen om fuld decentral koncern it-model drøftet.

Udvalget besluttede, at IT og ISDB-enheden skulle afklare aftalegrundlaget og samarbejdsorganisationen mellem koncernen og Statens It nærmere, idet der var uklarhed om status for den ISM kundeaftale med Statens IT, som SDS angiver at være aftaleholder på i notat vedr. Fuld decentral koncern it-model.

IT-chefen har siden udvalgets møde i februar meddelt Statens It og SDS, at departementet fremover deltager i Statens It's Kundestrategiske Forum, hvor den strategiske udvikling af Statens It drøftes blandt de tilsluttede ministerområder. SDS har hidtil repræsenteret koncernen i dette forum.

SDS vil fortsat repræsentere koncernen i Statens IT's Kundeforum, som bl.a. har til opgave at følge op på Statens It's drift samt at drøfte emner af tværgående karakter.

Derudover er ISDB-enheden og SDS i regi af CID-koordinationsforum i færd med at udarbejde notat om governance, roller og ansvar for den koncernfælles infrastruktur og it-services. Aftalegrundlag og samarbejdsorganisation mellem institutionerne i koncernen og Statens It vil indgå i dette notat, som forventes drøftet i udkastform på møde i CID-koordinationsforum den 31. maj 2024.

Efter beslutning i Digitaliseringsboardet den 22. februar 2024 er SDS er desuden ved at udarbejde et oplæg om systemejerskab og kontraktejerskab fsva. de koncernfælles systemer, som har haft driftstyregrupper (CRM, Public 360, WorkZone I og II samt Koncern Intra). Oplægget vil også rumme forslag til den fremtidige koordinering af koordinering af de tværgående systemer, som anvendes af mere end en institution (Bluewhale, FirstAgenda, Strålfors og Samwin). Oplægget forventes drøftet på møde i Digitaliseringsboard den 30. maj 2024.

Videre proces
Implementeringen af den ændrede koncern it-model pågår og drøftes ultimo maj 2024 i hhv. Digitaliseringsboard og CID-koordinationsforum. ISDB-enheden vil løbende holde CID-udvalget orienteret om status.

ABKN indledte med at bemærke, at der er stort fokus på punktet i koordinationsforum som også nævnt under punkt 8.b.

ABKN oplyste videre, at ISDB-enheden i samarbejde med SDS, er i gang med at udarbejde et notat, der forventes at være færdigt til behandling på mødet i CID-koordinationsforum den 20. juni 2024. CID-udvalget vil blive orienteret herom.

Beslutning
Udvalget tog orienteringen til efterretning.

9. Eventuelt

CLSO indledte med at spørge om der er punkter til eventuelt.

- CLSO gav ordet til SAK, der oplyste, at hun ikke længere ville være en del af udvalget, da hun stopper i departementet ved udgangen af måneden. ABKN tilføjede, at der er slået en DPA-stilling op, som ønskes besat senest 1. august 2024.
- SAK tilføjede, at oplysningsteksten til www.ism.dk, der blev godkendt under udvalgsmødet den 29. februar 2024 dags dato er blevet lagt på hjemmesiden.

10. Næste møde

Afholdes den 10-09-2024 kl. 13:30-15:00.