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: 15-01-2024
Enhed: ISDB-enheden
Sagsbeh.: DEPFBG
Sagsnr.: 2023-5662
Akt-id.: 102999

Version: 1.0
Godkendt af: DBV
Gældende fra: 14-01-2024

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
13. december 2023

Deltagere

Medlemmer

Dorte Bech vizard (DBV), CISO, næstforperson
Carsten Grage (CG), IT
Mette Rye Andersen (MRAN), ISDB-enheden
Pernille Seaton (PSE), Intern Administration
Trine Brøbecher (TRBR), HR

Observatører

Helle Ginnerup-Nielsen (HGN), DPO DEP
Philip Joen Bujnoch (PBU), DPO Benchmarkingenheden

Sekretariat

Finn Boilesen Guldbæk (FBG), ISDB-enheden
Sanae Karroum (SAK), ISDB-enheden

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**

DBV bød velkommen til udvalgets deltagere. Hun orienterede om, at den kommende afdelingschef for Strukturel Sundhed, Cecilie Louise Svane Olesen, var forhindret i at deltage til dagens møde. Herefter præsenterede alle deltagere sig selv.

DBV oplyste, at udover udvalgets faste medlemmer og observatører, består udvalget af tre medlemmer, der vil blive indkaldt, når der er relevante punkter på dagsordenen. Det drejer sig om følgende personer:

- Ulrik André Bøgelund, repræsentant fra Presse og Kommunikation
- Katja Roitmann, repræsentant fra Beredskab og Smitsomme sygdomme
- David Tokarski, repræsentant fra Data, Infrastruktur og Cybersikkerhed.

Bilag
2.2 Medlemmer af CID-udvalget.

2. Præsentation af elementer i ledelsessystemet for cyber-, informationssikkerhed og databeskyttelse

DBV indledte og gennemgik kommissorium for CID-udvalget, som godkendt af DC 10. oktober 2023.

DBV gav ordet til FBG, som præsenterede elementer af ledelsessystemet baseret på ISO 27001 og ISO 27701 for cyber-, informationssikkerhed og databeskyttelse. Præsentationen gav en grundlæggende indflyvning til standarderne og de elementer, der indgår i et robust ledelsessystem (PowerPoint vedlagt referat).

Bemærkninger fra udvalget:

- DBV oplyste, at målsætningen er, at departementet bliver grøn på alle punkter i modenhedsmålingen i løbet af 2024.
- PBU anbefalede for så vidt angår modenhedsmålingen, at det første, der skal arbejdes på er retningslinjer for medarbejdere, hvad angår Informationssikkerhed. På denne måde vil den enkelte medarbejder vide, hvordan man skal agere i forskellige henseender, der har med Informationssikkerhed at gøre. FBG foreslog, at politikker og retningslinjerne indgår i on-boarding af nye medarbejdere. Udvalget bakkede op om forslagene fra PBU og FBG.

Konklusion: Orienteringen vedr. kommissorium og ledelsessystemet for informationssikkerhed blev taget til efterretning.

Indstilling
Det indstilles, at orienteringen om Kommissorium for CID-udvalget og præsentation af ledelsessystem for informationssikkerhed tages til efterretning.

Sagsfremstilling
Departementschefen har som øverste ansvarlige for cyber-, informationssikkerhed og databeskyttelse i departementet den 10. oktober 2023 godkendt Kommissorium for udvalg for cyber-, informationssikkerhed og databeskyttelse i Indenrigs- og Sundhedsministeriets departement (bilag 1.1).

Udvalgets ansvarsområde dækker departementet og Benchmarkingenheden. Kommissoriet beskriver udvalgets sammensætning, roller og opgaver. Udvalgets medlemmer fremgår af vedlagte bilag 2.2.

Alle statens institutioner skal implementere ISO 27001-standarden, herunder et ISO 27001-baseret ledelsessystem for informationssikkerhed. På koncernniveau er det endvidere besluttet, at kravstandarden ISO 27701 også skal efterleves.

På mødet vil Finn Guldbæk præsentere elementer i ledelsessystemet i henhold til ISO 27001 og ISO 27701 (præsentation medbringes på mødet).

Bilag
2.1 Kommissorium for udvalg for cyber-, og informationssikkerhed og databeskyttelse i departementet
2.2 Medlemmer af udvalget
2.3 Præsentation.

3. Politik for cyber-, og informationssikkerhed og databeskyttelse i departementet

DBV indledte med at orientere om, at ledelsessystemet, kommissorium for CID-udvalget og CID-politikken tilsammen udgør det grundlag, som CID-arbejdet baseres på i departementet.

MRA præsenterede CID-politikken, der var udarbejdet i af ISDB-enheden med væsentlige bidrag fra SUM-DPO. Politikken lægger op til konkrete målsætninger for udvalgets arbejde. De enkelte målepunkter foreslås foldet ud i en årlig handleplan, som sekretariatet med udvalgets godkendelse vil udarbejde udkast til frem mod næste møde.

Udvalget drøftede udkastet og havde følgende bemærkninger*:*

- PBU foreslog at lette administrationen ift. versioneringer af politikken ved at slette punkt 8 og i stedet lade det fremgå af udvalgets handleplan, at udvalget årligt tager stilling til evt. behov for at revidere politikken. Udvalget besluttede, at ændre ordlyden under punkt 8 til ”CID-politikken revideres ved større ændringer.”.

Konklusion: Med de faldne bemærkninger blev politikken godkendt.
CID-politikken forelægges direktionen til orientering.

Sekretariatet udarbejder udkast til handleplan for 2024 mhp. drøftelse ved næste møde i CID-udvalget.

Indstilling
Det indstilles, at udvalget drøfter og godkender udkast til politik for cyber-, informationssikkerhed og databeskyttelse.

Sagsfremstilling
Departementets politik for cyber-, informationssikkerhed og databeskyttelse vil udgøre en central del af departementets samlede ledelsessystem for cyber-, informationssikkerhed og databeskyttelse.

Med vedlagte udkast foreslås tre formål med politikken:

1) At fastlægge de overordnede rammer for arbejdet med cyber-, informationssikkerhed og databeskyttelse.
2) At fastlægge en række målsætninger for departementets CID-arbejde med et tidssvarende og tilstrækkeligt højt niveau.
3) At fastlægge ansvar og organisering vedr. cyber-, informationssikkerhed og databeskyttelse.

Desuden foreslås det, at der udarbejdes 1-årige handleplaner med konkrete initiativer og indsatser for CID-udvalgets arbejde. Dette for at understøtte arbejdet med at realisere målsætningerne (jf. punkt 2) og med henblik på at prioritere ressourcerne.

Den videre proces
Med udvalgets godkendelse vil sekretariatet frem mod næste møde udarbejde udkast til handleplan for 2024.

Bilag
3.1 Udkast til Politik for cyber-, informationssikkerhed og databeskyttelse (CID-politikken).

4. **Retningslinje for: Indberetning af sikkerhedshændelser**

DBV indledte med at bemærke, at overblik over sikkerhedshændelser er centralt ift. informationssikkerhed og databeskyttelse. Et overblik giver bl.a. mulighed for læring, og er væsentligt i forhold til ledelsesinformation.

FBG orienterede om, at der med udkast til ny retningslinje er tale om en opdatering af gældende retningslinjer for indberetning af sikkerhedshændelser i departementet.

Mette orienterede om status på dialogen med SIT i forhold til indberetning, opfølgning og information vedr. indberettede sikkerhedshændelser fra SIT. Der afventes afklaring med SIT om overblik og tilbagemelding til de informationssikkerhedsansvarlige på indberettede sikkerhedshændelser.

Udvalget drøftede udkastet til politikken og havde følgende bemærkninger:
- CG spurgte, om det er alle sikkerhedshændelser, der skal indberettes via SIT, herunder også brud foretaget i F2 eller andre fagsystemer. MRAN bemærkede, at det fra et brugerperspektiv kan være nemmest, hvis man ikke skal forholde sig til det konkrete it-system i forbindelse med. indberetning af hændelser, men der kan selvfølgelig være undtagelser fsva. fagsystemer.
- CG spurgte, hvor hurtigt SIT reagerer ift. at orientere departementet, hvis hændelser vedrører brud på persondatasikkerheden ift. 72 timers fristen. MRAN svarede, at de erfaringsmæssigt er hurtige og svarer indenfor et par timer.
- CG oplyste, at særlige retningslinjer gør sig gældende i CPR-enheden, da afdelingschef mfl. skal orienteres ved et eventuelt brud. Dette fremgår ikke af det udkast til retningslinjer, der blev fremlagt under dagens møde.

Konklusion:
CID-udvalget besluttede, at CG og PBU udarbejder supplerende bemærkninger, der gør sig gældende for indberetning af brud for CPR-enheden og evt. andre fagsystemer.

Bemærkningerne sendes til ISDB-sektionen, der opdaterer udkastet, som forelægges godkendes på næste CID-udvalgsmøde den 29. februar 2024.

Indstilling
Det indstilles, at retningslinjen godkendes.

Sagsfremstilling
Arbejdet med registrering, håndtering, evt. indrapportering, opfølgning og ledelsesinformation på sikkerhedshændelser, der kan have effekt på departements informationer og data i forhold til fortrolighed, integritet og tilgængelighed, er vigtigt for at nå målsætningerne med cyber-, informationssikkerhed og databeskyttelse.

For at gøre det så enkelt som muligt for brugerne tilstræbes princippet om SPOC (Single Point of Contact) ifm. hændelsesrapportering.

På grund af fortsat uklarhed i forhold til systemer, hvor departementer har driftsansvaret (driftsmodel 0 og i tilfælde hvor sikkerhedshændelsen ikke er tilknyttet til et system men til en handling) skal brugeren forsat informere ISDB-sektionen om afviste indberetninger og manglende accept ved telefonisk indberetning.

Efter overgangen til SIT har der været uklarhed i forhold til hændelsesindberetning og efterfølgende tilbagemelding til relevante personer i departementet. Der pågår drøftelser med SIT både på koncernniveau og lokalt i departementet i processer, der vil give tilstrækkelig information om hændelsesrapportering, identifikation af hændelsestyper og håndtering.

Med godkendelse af retningslinje for indberetning af sikkerhedshændelse vil princippet om SPOC efterleves.

Den videre proces
Med udvalgets godkendelse vil retningslinjen blive formidlet til medarbejderne på intranettet. Dialogen med SIT vedr. optimering af processer fortsættes, og udvalget vil løbende blive orienteret.

Bilag
4.1 Udkast til retningslinje: Indberetning af sikkerhedshændelser.

5. Foreløbige interne retningslinjer for brug af generativ AI i departementet

DBV indledte og præsenterede forslaget om at bruge Digitaliseringsstyrelsens interne retningslinjer frem til departementet evt. selv har udarbejdet andre.

DBV bemærkede, at CID-koordinationsforum har besluttet at videndele på området, men ikke at udarbejde koncernfælles retningslinjer.

Udvalget drøftede indstillingen med følgende bemærkninger:

- HGN bemærkede, at hun i CID-koordinationsforum har vejledt om, at brug af generative AI-tjenester som f.eks. ChatGPT bør forbydes, til der er fortaget de lovligheds- og risikovurderinger, som er påkrævede i henhold til GDPR, herunder ift. informationssikkerhed. HGN havde givet supplerende vejledning til departementet og bemærkede, at det udgør en "compliance risiko" at godkende brugen af sådanne tjenester, før der er foretages det fornødne ift. efterlevelse af GDPR.
- HGN understregede, at hun er enig i, at det er nødvendigt med interne regler, der regulerer brugen af denne type tjenester, og at der er behov for effektive awareness-tiltag, der sikrer, at alle medarbejdere ved, hvordan de skal forholde sig, uanset om anvendelsen tillades eller ej. Dette bl.a. med henblik på at sikre, at brugerne i hvert fald ikke aktivt uploader personoplysninger om andre.

- Der fulgte en kort drøftelse vedr. oplysninger om medarbejdere, som tilgår AI-værktøjer i arbejdssammenhæng via offentligt tilgængelige hjemmesider. HGN vejledte om, at departementet bl.a. har ansvaret for at sikre, at der er den fornødne hjemmel til eventuelle videregivelser af oplysninger om brugere i departementet til f.eks. systemudbydere, og at oplysningspligten skal iagttages.
- HGN bemærkede videre, at departementet, såfremt retningslinjerne tiltrædes, bør præcisere, hvad der i denne sammenhæng menes med sensitive oplysninger, herunder at begrebet omfatter alle, og ikke kun fortrolige, personoplysninger.
- DBV bemærkede, at Digitaliseringsstyrelsen bl.a. har til opgave at vejlede offentlige myndigheder på området, hvorfor det foreslås at bruge deres interne retningslinjer.

Konklusion:
Udvalget godkendte retningslinjerne som midlertidige retningslinjer med en præcisering af, hvad sensitive oplysninger er. Det blev samtidig besluttet, at ISDB-enheden sideløbende indleder et arbejde vedr. de nødvendige vurderinger.

Endelig blev det besluttet, at retningslinjerne formidles på næste chefmøde og til medarbejderne på intranettet i det nye år.

Indstilling
Det indstilles, at CID-udvalget godkender, at departementet på foreløbig basis anvender Digitaliseringsstyrelsens interne retningslinjer for brug af generativ AI. Dette frem til departementet har udarbejdet egne retningslinjer på området.

Sagsfremstilling
Generativ AI, som f.eks. ChatGPT, kan anvendes til mange formål, herunder også til løsning af visse opgaver i departementet. På nuværende tidspunkt har departementet ingen retningslinjer på området.

Digitaliserings og Ligestillingsministeriet er gået i gang med at udarbejde en vejledning til de statslige myndigheder omkring brug af generativ kunstig intelligens, men det er uvist, hvornår vejledningen udkommer.

Det foreslås på den baggrund at anvende Digitaliseringsstyrelsen interne retningslinjer for brug af generativ AI (bilag 5.1) frem til departementet har udarbejdet egne retningslinjer. I denne proces skal der tages højde for bl.a. juridiske og sikkerhedsmæssige aspekter ift. anvendelse og evt. udvikling af generativ kunstig intelligens i departementet.

Den videre proces
Med udvalgets godkendelse vil retningslinjerne blive formidlet til medarbejderne på intranettet og Direktionen vil blive orienteret om udvalgets beslutning.

Udvalget vil blive inddraget i det videre arbejde omkring retningslinjer for brug af generativ kunstig intelligens i departementet.

Bilag
5.1 Udkast til retningslinje: Brug af generativ AI i departementet.

6. **Proces for mødemateriale**

DBV præsenterede forslag til proces for mødemateriale.

Konklusion: Indstillingen blev godkendt.

Indstilling
Det indstilles, at proces for dagsorden godkendes.

Sagsfremstilling
Følgende proces foreslås ifm. indkaldelse af afholdelse af udvalgsmøder:

- Dagsordenspunkter kan meldes ind af alle medlemmer indtil 3 uger før mødets afholdelse
- Dagsorden og bilag udsendes 8 dage før mødets afholdelse
- Referat udsendes senest 14 dage efter mødets afholdelse
- Der afholdes 4 møder årligt. Yderligere møder kan indkaldes ved behov.

Når et medlem af udvalget indmelder et punkt, er medlemmet automatisk ansvarlig for punktet samt fremlæggelse på selve mødet.

7. Brev vedr. Justitsministeriets fortolkning af retningslinjer for statslige myndigheders opbevaring af slettede e-mails.

PSE orienterede om SUM status og CG orienterede om IM status på efterlevelse af retningslinjerne for opbevaring af slettede mail.

DBV opsummerede, at systemejerskabet for mailløsningen for SUM delen ligger hos PSE og for IM delen hos CG.

Begrebet systemejer defineres nærmere i 2024 i forbindelse med afklaring af roller og ansvar, jf. CID-politikken.

Konklusion: Orienteringen blev taget til efterretning. ISDB-sektionen fordeler brevet til de underliggende myndigheder.

Indstilling
Det indstilles, at orienteringen tages til efterretning og ansvar for opfølgning placeres hos systemejer for mailsystemet.

Sagsfremstilling
Justitsministeriet oplyser, at slettemarkerede e-mails i statslige myndigheders hoved- og funktionspostkasser og deaktiverede hoved- og funktionspostkasser bør opbevares i 5 år.

Opbevaringsfristerne er på 5 år for medarbejdere, 10 år for chefer og 25 år for særlige rådgivere, departementschefer og ministre.

De samme frister er gældende i klassificerede e-mailsystemer. Opbevaring af klassificerede e-mails vil fortsat skulle ske i overensstemmelse med sikkerhedscirkulæret.

Bilag
7.1 JM orienteringsbrev vedr. opbevaring af slettede e-mails mv.

8. **Mødeplan for 2024**

Konklusion: Datoerne blev godkendt.
Dagsordenspunkter til næste møde kan meldes ind af alle medlemmer frem til og med onsdag den 8. februar 2024.

Indstilling
Dat indstillet af de 4 datoer godkendes
29-02-2024
23-05-2024
10-09-2024
13-11-2024

Næste møde
Torsdag den 29. februar 2024 kl.: 13:30-15:00

9. **Eventuelt**

DBV orienterede om, at BES har udarbejdet udkast til beredskabsplan for departementet.

DBV bemærkede, at IT-beredskabsplanen bør være en del af beredskabsplanen og foreslog, at IT-chefen sikrer dette (PSE og CG følger op).

ISDB-enheden og BES mødes med henblik på at indarbejde evt. øvrige udeståender ift. Kravs standarder for så vidt angår informationssikkerhed.

DBV takkede for et godt møde.