

Søjle 1

Forslag om oprettelse af enhed til håndtering af særlige risikogrupper

Navneforslag:

National Enhed for Koordination af Sikkerhedsrelevant Information og Data (NEKSID).

Resortministerium (forslag, rækkefølge):

1. Statsministeriet
2. Ministeriet for Samfundssikkerhed og Beredskab

Formål 1:

Samkørsel af data, opbevaring af data, registerføring af data, behandling af data, samt analyse af data, fra:

- Forsvarets Efterretningstjeneste
- Center for Cybersikkerhed
- Politiets Efterretningstjeneste
- Hærens Efterretningsregiment
- Passenger Name Record (Politiets Passagerlistoplysninger)
- Skattestyrelsen (Eks, Person – Udland – Udland 8); TS-Tele
- National enhed for Særlig Kriminalitet

Formål 2:

- Drift, vedligeholdelse, og varetagelse af dataregistre med data indhentet fra de i Formål 1 beskrevne organisationer.
- Særligt hjemmel til at opbevare, behandle, og ved de i Formål 3 beskrevne situationer, videregive data til de i Formål 1 beskrevne organisationer, efter behov.
- Særligt hjemmel til, at opbevare data uden tidsbegrænsning, uden orientering af personer i dataregistre, og uden orientering af personer ved behandling, eller videregivelse af data.

Formål 3:

Videregivelse af data til i formål 1 nævnte, ved mistanke om:

- Overtrædelse af Strafferetsmæssige forhold.
- Tilknytning til af EU eller Danmark beskrevne fremmede, fjendtlige, eller terrorliste-forbundende personer, organisationer, eller netværk.
- Sabotage, obstruktion, kollaboration, spionage, eller terrorvirksomhed, målrettet danske eller EU interesser.

Formål 4:

Overvågning af:

- Personer i Gruppe E & F, beskrevet i Risikogruppermatricen for NEKSID (Søjle 1a).
- Spioner, fremmede agenter, fremmede aktører, terrorister, m.v.

Formål 5:

Udvikling af analyser og vurderinger af risikobilleder vedrørende:

- Brand og Redning
- Politivirksomhed og Sikkerhed
- Sundhed og ABC

Søjle 1a

Risikogruppermatrice for NEKSID

Risikofaktorer af Sikkerhedsbehov.

Risikofaktorer altid højeste Type ved tvivl.

Risikogrupper:

Faktorgruppe A: 0 = Ingen interesse.

Faktorgruppe B: 1-4 = Laveste interesse.

Faktorgruppe C: 5-8 = Middel-lav interesse (Fortrolig Godkendelse anbefales, Løbende kontrol af omgangskreds og økonomiske forhold i laveste indsats).

Faktorgruppe D: 9-12 = Middel interesse (Hemmelig Godkendelse anbefales, Løbende kontrol af omgangskreds og økonomiske forhold i aktiv indsats).

Faktorgruppe E: 13-20 = Høj interesse (Yderst Hemmelig Godkendelse anbefales, Løbende kontrol af omgangskreds og økonomiske forhold i aktiv forebyggende indsats).

Faktorgruppe F: 21+ = Højeste interesse (Yderst Hemmelig Godkendelse anbefales, løbende kontrol af omgangskreds og økonomiske forhold i aktiv målrettet indsats).

Kommentar 1: Såfremt at en Faktor udelukkende skyldes en enkelt Type, se eksempelvis:

Vektor 1 = 1

Vektor 2 = 4

Faktor = $1 \times 4 = 4$

Bør personens stilling flyttes en faktorgruppe op, her eks fra Faktorgruppe B til C.

Kommentar 2: Såfremt at en Vektor er 3 eller over, mens den anden Vektor er 0, bør det følge at:

Vektor 3 = Tjenesteformål

Vektor 4 = Fortrolig

Vektor 5 = Hemmelig

Vektor 6 = Yderst Hemmelig

Eksempel 1:

Person A har følgende oplysninger.

Person A er rengøringsassistent, ansat af Kommune X, eller af Virksomhed Y som leverer rengøring til Kommune X, i en tilfældig klynge af børnehaver.

Person A har til dagligt i følge med sit arbejde adgang til en klynge af børnehaver.

Derfor har Person A en Vektor 1 = 1.

Person A har adgang til et lokalt Mandskabsplanlægningssystem, men ingen yderligere informationssystemadgang.

Derfor har Person A en Vektor 2 = 0

$Vektor\ 1 \times Vektor\ 2 = 1 \times 0 = 0$.

Person A er derfor ikke interessant i sig selv at undersøge eller profilere, givet Person As' adgange.

Eksempel 2:

Person B har følgende oplysninger.

Person B kommer i en række forskellige matrikler ejet af Skattestyrelsen, som følge af sit arbejde, men kommer ikke (normal vis) i selve Skatteministeriet.
Derfor har Person B en Vektor 1 = 5.

Person B er kontorchef i Skattestyrelsen, og har som følge af sit arbejde en række adgange som bruger i en række af Skattestyrelsens systemer. Disse systemer er særligt følsomme, og adgangen betyder, at Person B har stor mulighed for, at påvirke individuelle eller flere personer, og samfundet i helhed, gennem sin adgang.
Derfor har Person B en Vektor 2 = 5.

Vektor 1 x Vektor 2 = 5 x 5 = 25.

Person B bør derfor have en Yderst Hemmelig godkendelse, til at varetage sit arbejde, og er særligt interessant for PET at holde øje med.

Vektor 1: Person med faglig adgang til Offentlige Faciliteter.

Type 0

Adgang til enkelt matrikel uden sikkerhedsinteresse.

Eks: Skole, Børnhave, eller lignende

Type 1

Adgang til klynge af matrikler uden sikkerhedsinteresse.

Eks: Skoleklynger, Børnehaveklynge, Plejehjemsklynge, m.v.

Type 2

Adgang til matrikel af laveste sikkerhedsinteresse.

Eks: Brandstation, Lokal Politistation, Lokal TV Station, eller lignende.

Type 3

Adgang til matrikel af middel-lav sikkerhedsinteresse, eller adgang til flere matrikler af laveste sikkerhedsinteresse.

Eks: Central brandstation, central politistation, militærbase med værnepligtige uden særlig funktion, styrelser under ministerier som ikke er i Type 5.

Type 4

Adgang til matrikel af middel sikkerhedsinteresse, eller adgang til flere matrikler af middel-lav sikkerhedsinteresse.

Eks: Folketinget, Ministerier (Eksklusiv Finansministeriet, Forsvarsministeriet, Justitsministeriet, Ministeriet for Samfundssikkerhed og Beredskab, Statsministeriet, Skatteministeriet), Styrelser under Type 5 ministerier, Militærbase eller Militærinstallation af sikkerhedsinteresse.

Type 5

Adgang til matrikel af middel-høj sikkerhedsinteresse, eller adgang til flere matrikler af middel sikkerhedsinteresse.

Eks: Finansministeriet, Forsvarsministeriet, Justitsministeriet, Ministeriet for Samfundssikkerhed og Beredskab, Statsministeriet, Skatteministeriet, FE/PET/NSK matrikler, Dataopbevaringsmatrikler, NATO/EU Militæroperative Installationer.

Type 6

Adgang til matrikel af høj sikkerhedsinteresse, eller adgang til flere matrikler af middel-høj interesse.

Eks: NATO/EU/DK operative kommandoer, Datacentraler, FE/PET/NSK hovedkvarterer, eller lignende.

Vektor 2: Person med faglig adgang til Offentligt Informationssystem

Type 0:

Adgang til lokalt informationssystem som bruger.

Eks: AULA (bruger), Mandsskabsplanlægning (brugeradgang), Fællesdrev (eks. i en børnehave).

Type 1:

Adgang til lokalt informationssystem som leder, jurist, eller økonom.

Eks: Budgetsystem til lokalt plejehjem/skole/børnehave eller lignende, HR-system til lokalt plejehjem/skole/børnehave, Mandsskabsstyring i lokalt plejehjem/skole/børnehave, m.v.

Type 2:

Adgang til kommunalt informationssystem eller ikke samfundskritisk informationssystem.

Eks: Kommunal budget/økonomisystem, kommunal ledelsessystem, kommunal fællesdrev, m.v., af ikke sikkerhedsmæssig interesse,

Type 3:

Adgang til fler-kommunalt informationssystem eller regionalkritisk informationssystem. (Sikkerhed- eller Forsvarssystemers Administratorer).

Eks: Regionernes interne dataregistre, system der påvirker drift af flere kommuners daglige driftsopgaver, økonomistyringssystemer, juridiske styringssystemer, m.v.

Type 4:

Adgang til statslige driftssystemer som ikke påvirker kritisk infrastruktur, eller adgang til datasystemer som påvirker samfundsvigtige virksomheder. (Sikkerhed- eller Forsvarssystemers Programmører).

Eks: Novo driftssystemer, Maersk driftssystemer, bankvirksomheders driftssystemer, styrelser driftssystemer, sundhedssektorens driftssystemer, politiets driftssystemer, brand- og redningstjenesternes driftssystemer, forsvarets driftssystemer.

Type 5:

Adgang til statslige driftssystemer som påvirker kritisk infrastruktur, eller adgang til datasystemer som påvirker samfundskritiske virksomheder. (Sikkerhed- eller Forsvarssystemers Ingeniører).

Eks: Operative driftssystemer, infrastrukturkritiske driftssystemer, samfundskritiske driftssystemer.

Type 6:

Administrator eller programmør adgang til statslige driftssystemer eller datasystemer som påvirker samfundsvigtige til samfundskritiske virksomheders evne til at drifte. (Sikkerhed- eller Forsvarssystemers Systemejere).

Søjle 2

Oprettelse af Nationalt Akademi for Uddannelser i Beredskab, Indsats, og Sikkerhed

Navneforslag:

Nationalt Akademi for Uddannelser i Beredskab, Indsats, og Sikkerhed (NAUBIS).

Resortministerium (forslag, rækkefølge):

1. Ministeriet for Samfundssikkerhed og Beredskab
2. Indenrigsministeriet
3. Forsvarsministeriet

Formål 1:

- Drift, udvikling, og implementering af uddannelser inden for:
 - Brand- og Redningstjeneste
 - Politi- og Sikkerhedstjeneste
 - Sundheds- og ABC-tjeneste
 - Indsatsledelse
 - Indsats ved Intentionel Menneskeskabt Trussel
 - Forebyggelsesindsats
 - Øvelser & Træning

Formål 2:

- Drift, udvikling, og implementering af uddannelser inden for:
 - Tværsektoriel tjeneste
 - Tværsektoriel indsats
 - Efterretningstjeneste
 - Kontrafterretningstjeneste
 - OSINT
 - Dataanalyse
 - Systemanalyse
 - Organisationsanalyse
 - Netværksanalyse
 - Strukturel Analyse

Formål 3:

- Drift, udvikling, og implementering af uddannelser inden for:
 - Driftsledelse
 - Teamledelse
 - Organisationsledelse
 - Taktisk Ledelse
 - Strategisk Ledelse
 - Efterretningsledelse
 - Netværksledelse
 - IT-ledelse
 - Informationssikkerhedsledelse

Formål 4:

- Drift, udvikling, og implementering af uddannelser inden for:
 - Civilsektor – Militærsektor Indsats og Samarbejde
 - Civilsektor – Efterretningssektor Indsats og Samarbejde
 - Civilsektor – Sikkerhedssektor Indsats og Samarbejde
 - samt Kombinatorisk Indsats og Samarbejde

Formål 5:

- Drift af Analyse, Læring, Udvikling, og Videnscenter (ALUV)

Søjle 2a

Strukturelt forslag til NAUBIS

Geografisk/Organisatorisk Strukturforslag:

- Hovedkvarter placeret et ikke offentligt kendt sted.
- NAUBIS "Geografisk"/"Strukturel" Koncernopdeling
 - NAUBIS Øst (Sjælland, Bornholm, Lolland, Falster)
 - NAUBIS Vest (Jylland, Fyn)
 - NAUBIS Færøerne/Grønland
 - NAUBIS Maritim (Aalborg, Gilleleje/Frederiksværk, Langeland)
 - NAUBIS Ledelse & Organisation
 - NAUBIS Efterretning & Sikkerhed
 - NAUBIS Analyse, Data, & IT
 - NAUBIS Analyse, Læring, Udvikling, og Videnscenter (ALUV)
- NAUBIS ALUV (Aalborg, Odense, & Helsingør)
- NAUBIS placering af "Træningsbaser"/"Uddannelsescentre"
 - Grønland og/eller Færøerne
 - Sjælland, Bornholm, Lolland, Falster
 - Holmen, København
 - Nordsjælland
 - Vestsjælland
 - Gedser
 - Rødby
 - Rønne
 - Fyn
 - Odense
 - Svendborg
 - Langeland
 - Jylland
 - Esbjerg
 - Aalborg
 - Aarhus
 - Sønderborg

Søjle 3

Styrkelse af Forebyggelseskapacitet vedrørende Forsvarets Efterretningstjeneste, Hærens Efterretningsregiment, og Skattestyrelsen

Navneforslag:

Ikke relevant, da denne søjle omhandler en øget beføjelse til FE, HER, og Skattestyrelsen.

Resortministerium (forslag):

Ikke relevant, da FE, HER, og Skattestyrelsen allerede nu er placeret under ministerier.

Kommentar: Denne søjle er beskrevet uden stillingstagen til søjlerne 1 og 2.

Formål 1:

- Forsvarets Efterretningstjeneste tilføres følgende myndighedsopgaver:
 - Overvågelse af Beredskabs-, Forsvars- og Sikkerhedsrelaterede danske nationale forvaltningsorganisationer, eller disses underorganisationer, samt fysiske personer ansat ved disse danske nationale forvaltningsorganisationer, eller disses underorganisationer. Disse tydeliggøres i Søjle 3a.
 - Overvågelse af juridiske personer, samt fysiske personer, som indgår i samarbejdsrelationer, som leverandører, eller som aftagerer af ydelser fra i Søjle 3a nævnte danske forvaltningsorganisationer.

Formål 2:

- Opbyggelse, varetagelse, drift, og vedligehold af dataregistre omhandlende fysiske eller juridiske person af interesse, som beskrevet i Formål 1 & 3.
- Opbevaring og behandling af disse data i mindst 10 år fra data er registreret.

Formål 3:

- Identificering af fysiske eller juridiske personer, som har en eller kan have en kritisk indflydelse på, IT-systemmæssig adgang til, eller personlig eller økonomisk interesse i, at yde negativ indflydelse på danske kapaciteter til at føre effektivt forsvar, beredskab, sundhedsindsats, sikkerhedsindsats, eller politivirksomhed.

Formål 4:

- Videregivelse af saglige eller væsentlige data omhandlende de i Formål 1 eller 3 beskrevne fysiske eller juridiske personer, til Politiets Efterretningstjeneste, National enhed for Særlig Kriminalitet, Politiet, og/eller Anklagemyndigheden, med henblik på forebyggende eller aktiv indsats.

Formål 5:

- Hærens Efterretningsregiment tilføres myndighedsopgave at videregive data som beskrevet i Formål 1 eller 3, til Forsvarets Efterretningstjeneste.

Formål 6:

- Skattestyrelsen tilføres myndighedsopgave at videregive data som beskrevet i Formål 1 eller 3, til Forsvarets Efterretningstjeneste, hvis der er risiko for, at denne data kan betragtes som væsentlig, for Forsvarets Efterretningstjeneste, Politiets Efterretningstjeneste, og/eller National enhed for Særlig Kriminalitet.

Søjle 3a

Liste over danske forvaltningsorganisationer, som kan påvirke eller yde indflydelse på Danmarks forvaltningsorganisationer, hvis myndighedsopgaver omfatter: beredskabsvirksomhed, efterretningsvirksomhed, finansielle sikkerhedsvirksomhed, forsvarsvirksomhed, politivirksomhed, redningsvirksomhed, sikkerhedsvirksomhed, og sundhedsvirksomhed.

UDFYLDES AF RETSUDVALGET / RETSUDVALGSMEDLEMMERNES KONTORER