HJEMMEVÆRNSKOMMANDOBESTEMMELSE

Emne:
Bestemmelse om behandling af personoplysninger i Hjemmeværnet

Ref.:
a. Databeskyttelsesloven lov nr. 502 af 23/5/2018.
b. FMNBST 280-1, Bestemmelse om fordeling af dataansvar, herunder fastlæggelse af fælles dataansvar, mellem myndigheder i Forsvarsministeriets koncern
c. FMNBST 280-2, Bestemmelse om håndtering af brud på persondatasikkerheden i Forsvarsministeriets koncern.
d. FMNBST 400-1, Bestemmelse om mærkning og håndtering af personoplysninger, der skal mærkes "PERSONOPLYSNING, FORTROLIG – POF".
e. Cirkulære 9014 af 10/01/2017 om Hjemmeværnets inddeling
f. FMIBST 380-02, Bestemmelse for Forsvarsministeriets IT-tjenesteudvalg
g. Vejledning og skabeloner på HJV.dk, under fagområdet Databeskyttelseslovens område, og på KFI på siden Persondataforordningen (GDPR)

Bilag:
1. Hjemmeværnets driftsorganisation for GDPR
2. Indberetningsskema for decentrale systemer, tjenester og processer

1. GENERELT
Denne bestemmelse gælder for alle fastansatte og frivillige i Hjemmeværnet.

I denne bestemmelse fastsættes reglerne for behandling af personoplysninger i Hjemmeværnet som helt eller delvist foretages ved hjælp af automatisk databehandling, samt anden ikkeautomatisk (manual) behandling af personoplysninger, der er eller vil blive indeholdt i et register med forbehold for undtagelserne i gældende lovgivning (ref. a).

Fordeling af dataansvaret og retningslinjerne for behandling af personoplysninger i Forsvarsministeriets koncern fremgår af ref. b., c. og d.

2. OPGAVEFORDELING
Efterlevelse af databeskyttelsesloven i Hjemmeværnet tager udgangspunkt i Hjemmeværnets driftsorganisation for GDPR (bilag 1).

2.1. Databeskyttelsesrådgiver (DPO)
Hjemmeværnet har en DPO, som fungerer for alle Hjemmeværnets dataansvarlige myndigheder (se pkt. 2.2).

Ved enhver tvivl om efterlevelse af databeskyttelsesloven i Hjemmeværnets behandling af personoplysninger skal DPO konsulteres herom.

2.1.1. DPO opgaver
DPO opgaver er defineret i databeskyttelsesforordningens bilag 1, artikel 39 (ref. a). Dette inkluderer bl.a., at:

- være Hjemmeværnets POC over for Datatilsynet,
- rådgive de dataansvarlige myndigheder, ansatte og frivillige vedrørende behandling af personoplysninger,
- overvåge overholdelsen af databeskyttelsesreglerne, fx gennem ad hoc deltagelse i Hjemmeværnskommandoens tilsyns- og inspektionsvirksomhed,
- rådgive i forbindelse med udarbejdelse af konsekvensanalyser,
- støtte til vedligeholdelse af fortegnelser over behandlingsaktiviteter i samarbejde med de enkelte dataansvarlige myndigheder,
- modtage underretning om og rådgive Hjemmeværnet i forbindelse med brud på persondatasikkerheden jf. pkt. 5.,

DPO kontaktoplysninger:
E-mail: hjk-ktp-dpo@mil.dk
Telefon: +45 72 82 00 16
Ved brev: Hjemmeværnskommandoen, ATT: databeskyttelsesrådgiver, Sankelmarksvej 26, 4760 Vordingborg

Ved Hjemmeværnets DPO forfald overtager nærmeste chef for DPO opgaverne omfattet af punkt 2.1.1.

2.2. Dataansvarlig
Fordelingen af det selvstændige dataansvar i Hjemmeværnet følger Cirkulære 9014 af 10/01/2017 om Hjemmeværnets inddeling (ref. e).

De seks dataansvarlig myndigheder er:
- Hjemmeværnsstaben
- Marinehjemmeværnet
- Flyverhjemmeværnet
- Landsdelsregion Vest
- Landsdelsregion Øst
- Hjemmeværnsskolen

2.2.1. Dataansvarets omfang
Marinehjemmeværnet, Flyverhjemmeværnet og Landsdelsregionernes dataansvar omfatter foruden egen myndighed alle underlagte myndigheder. Hjemmeværnsledelsen omfattes af Hjemmeværnsstabens dataansvar.

2.2.2 Awareness træning
Den enkelte dataansvarlige myndighed har ansvaret for uddannelse og awareness i databeskyttelse. Det er et krav for alle frivillige og fastansatte at gennemføre FELS kurset Informations- og persondatasikkerhed i Hjemmeværnet. POC GDPR og P-personel skal tillige tage FELS kursus i Databeskyttelse. Materiale til supplerende uddannelse og awarenesstræning findes på HJV.DK og på KFI (ref. g). Hjemmeværnets DPO kan kontaktes for støtte til myndighedsspecifik awarenesstræning og uddannelse.

2.3. BEHANDLINGSGRUNDLAG
Den enkelte dataansvarlige myndighed har ansvaret for at sikre dokumentation for at behandling af personoplysninger sker i overensstemmelse med gældende lovgivning.

2.3.1. Dataansvar
Det er myndighedschefens ansvar at drage omsorg for, at databeskyttelsesloven efterleves inden for eget ansvarsområde herunder bl.a. i relation til procedurer, bestemmelser, uddannelser og vejledninger.

2.3.2. FÆLLES DATAANSVAR
Aftaler vedrørende fælles dataansvar reguleres i særskilte bestemmelser og aftaler.

2.4 KONTAKTPERSON (POC)
De dataansvarlige myndigheder, jf. punkt 2.2, samt afdelingerne ved hjemmeværnsstaben skal til enhver tid have udpeget en POC GDPR, hvormed DPO kan koordinere.

POC GDPR skal meldes ind til DPO via FIIN mail til: HJK-KTP-DPO.

3. IT-SYSTEMER, TJENESTER OG MANUELLE PROCESSER
Forud for anskaffelsen af IT-systemer, tjenester og lignende, samt iværksættelse af manuelle processer (ikkeautomatiske processer) skal DPO inddrages med henblik på efterlevelse af de databeskyttelsesretslige regler.

For de ikke koncernfælles IT-systemer og tjenester i Hjemmeværnet ligger forretningsansvaret (ref. f) ved myndighedschefen, eller afdelingschefen hvor systemet/tjenesten er forankret.

3.1. RAPPORTERING TIL DPO
Den dataansvarlige myndighed skal holde DPO løbende ajour med status for IT-systemer/-tjenester og lignende han/hun er ansvarlig for ved at indsende ajourført Indberetningsskema for decentrale systemer, tjenester og processer (bilag 2).

3.2. Registrering af ikkeautomatisk (manuel) behandling af personoplysninger
Myndighedschefen er ansvarlige for at holde DPO løbende ajour med status for myndighedens ikkeautomatiske (manuelle) behandling af personoplysninger ved at indsende Indberetningsskema for decentrale, tjenester og processer (bilag 2).

3.3. MILSIK ORGANISATION
Som led i arbejdet med militærsikkerhed understøtter MILSIKOF og CH UAFD (som ansvarlig for militærsikkerhed ved UAFD) efterlevelsen af persondataloven. Konkret sker dette ved at medtage principperne for behandling af personoplysninger i det tilsyn der udføres.

3.4. IT SIK ORGANISATION
Som led i efterlevelsen af koncernens IT-sikkerhedsregler bl.a. ISO 27001 standarden, understøtter Hjemmeværnets IT-sikkerhedsorganisation databeskyttelseslovens krav til sikring af IT-systemer/tjenester hvori der behandles personoplysninger.

3.5. RISIKOVURDERING (PIA - Privacy Impact assessment)
Den dataansvarlige myndighed har ansvaret for, at der udarbejdes en PIA i relation til enhver behandling af personoplysninger. Risikovurderingen skal høres ved DPO før behandlingsaktiviteten igangsættes. PIA arkiveres ved den dataansvarlige myndighed.

3.6. KONSEKVENSANALYSE (DPIA - DATA PROTECTION IMPACT ASSESSMENT)
Den dataansvarlige myndighed har ansvaret for, at der udarbejdes en konsekvensanalyse[1] (DPIA) i relevant omfang. DPIA skal høres ved DPO før behandlingsaktiviteten igangsættes. DPIA arkivers ved den dataansvarlige myndighed.

4. VEJLEDNINGER
Opdaterede vejledninger, skabeloner, højere myndigheders bestemmelser m.v. findes på HJV.DK og på KFI (ref. g).

[1] Se nærmere på HJV.dk og KFI ref. g

4.1. SAMTYKKEERKLÆRING
Et samtykke kan udgøre et gyldigt hjemmelsgrundlag, men bør kun anvendes hvis der ikke findes anden hjemmel. I tilfælde af tvivl skal DPO inddrages.

5. REGISTREREDES RETTIGHEDER
Retningslinjer for besvarelse af henvendelser fra registrerede vedrørende databeskyttelsesretlige rettigheder findes på KFI, jf. ref. g.

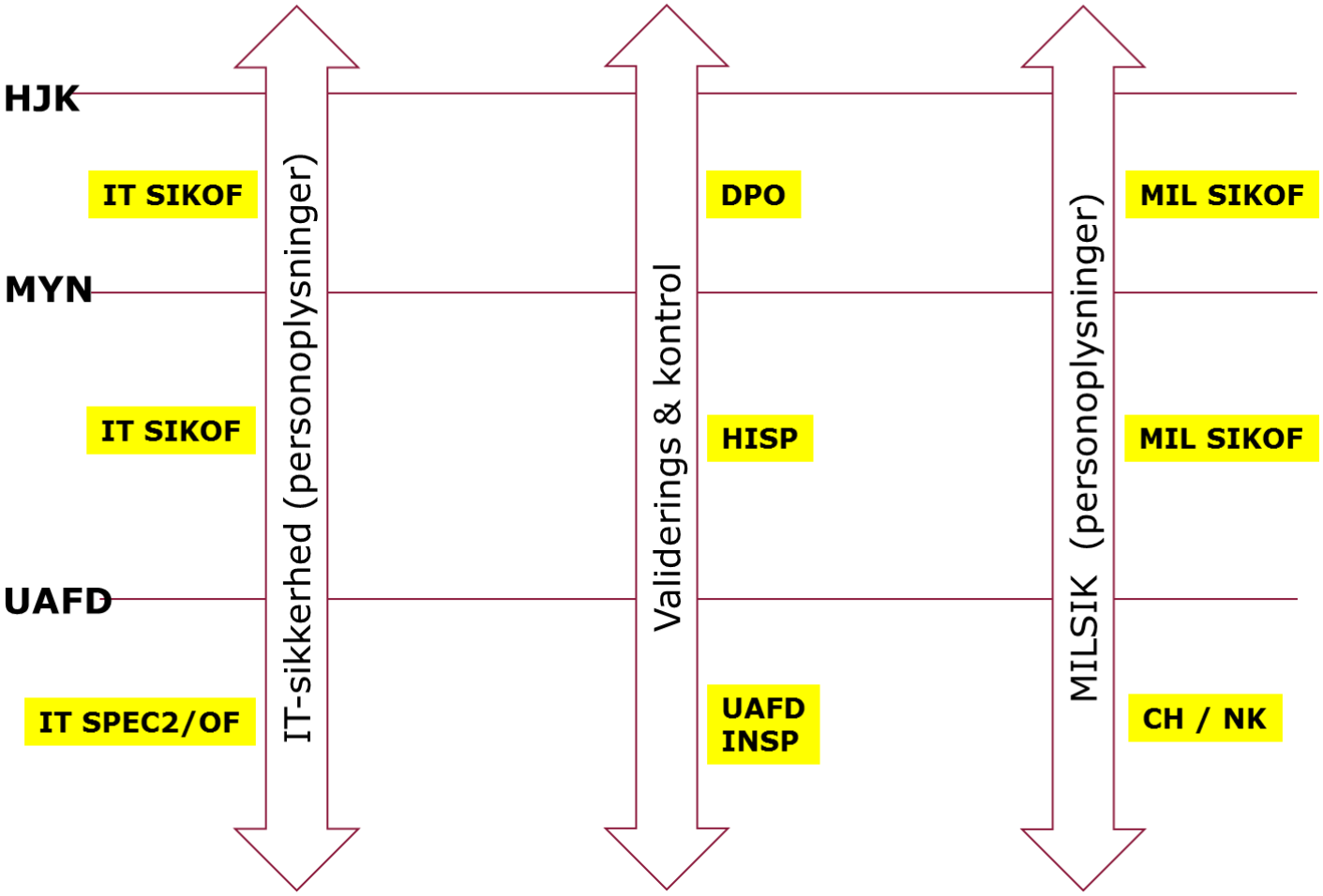
6. BRUD PÅ PERSONDATASIKKERHEDEN
Retningslinjer for håndtering af brud på persondatasikkerheden findes på KFI, jf. ref. g.

7. SAGSBEHANDLER
Ledelsessekretariatet, hjemmeværnskommandoen.

HJEMMEVÆRNET

Hjemmeværnets driftsorganisation for GDPR

3 driftspor



[1] NK forestår UAFD administration og forvaltning inden for områderne; Materiel, Personel og Økonomi.

Ordliste

CH	- Chef
DPO	- Data Protection Officer (Databeskyttelsesrådgiver)
GDPR	- General Data Protection Regulation (Databeskyttelsesforordningen)
HISP	- Helhedsinspektion (forvaltningsinspektion af Hjemmeværnets myndigheder)
HJK	- Hjemmeværnskommandoen
INSP	- Inspektion
ITOF	- Informationsofficer
IT-SPEC2	- Informationsspecialist 2
IT SIKOF	- Information teknologi sikkerhedsofficer / Informationssikkerhedsofficer
SIKOF	- Sikkerhedsofficer for den militære sikkerhedstjeneste
MYN	- Myndighed

HJEMMEVÆRNET

Indberetningsskema for decentrale systemer, tjenester og processer

Formål: Med baggrund i HJKBST 400-210, Bestemmelse om behandling af personoplysninger i Hjemmeværnet, skal den dataansvarlige myndighed holde DPO og HJK IT-sikkerhedsansvarlige løbende ajour med status for it-systemer/-services , som myndigheden er ansvarlig for, ved at indsende dette skema via FIIN mail til: HJK-KTP-DPO.

Dato	*Angiv dato for indberetning/opdatering.*	
System / tjenester / process / behandling	*Angiv navn på system/tjeneste/process/behandling. Denne rubrik vedrører både behandling af personoplysninger i IT-systemer/tjenester samt fysiske registre.*	
Dataansvarlige myndighed		
Dette skemas udfærdigende sagsbehandler	*Stabsnummer.*	
Formål	*Angiv formål med system, med angivelse af hvilket overordnet formål fra myndighedens fortegnelse over behandlingsaktiviteter det understøtter.*	
Sikkerhedsforanstaltninger	*En generel beskrivelse af de tekniske og organisatoriske (fysiske) sikkerhedsforanstaltninger, f.eks. Angivelse af hvorvidt ISO 27001 er opfyldt herunder om ISI del 2 er udarbejdet, evnen til at sikre vedvarende fortrolighed, integritet og robusthed.*	
Bliver data i dette system behandlet af andre dataansvarlige?	*Ja/Nej - i givet fald hvilke myndigheder?*	
Leverandører (Databehandler)	*Angiv navn og kontaktoplysninger på leverandør.*	
Databehandleraftale	*For systemer/tjenester hvori der behandles personoplysninger af en tredjemand, skal der udarbejdes en databehandleraftale. Angiv dato for seneste databehandleraftale her, og vedlæg kopi af databehandleraftalen. Filen navngives "Databehandleraftale_>System-/Servicenavn<_>dato<" f.eks. "Databehandleraftale_HJV.dk_10SEP18". Den koncernfælles skabelon for databehandleraftaler ligger på KFI Persondataforordningen (GDPR).*	