Ert tjänsteställe, handläggare | Ert datum | Er beteckning

Vårt tjänsteställe, handläggare | Vårt föregående datum | Vår föregående beteckning

Zenobia Rosander och Stefan Styrenius,
MUST SÄKK SÄKS INFOSÄK
Anders Wiklund, JURS

# Säkerhetskrav på IT-system som är avsedda för behandling av personuppgifter

## Bakgrund

När Försvarsmakten utvecklar ett IT-system så ska bl.a. en verksamhets- och regelverksanalys[1] tas fram. I verksamhetsanalysen ska det bl.a. identifieras om IT-systemet kommer att behandla personuppgifter. I regelverksanalysen redogörs sedan för vilka författningar som är tillämpliga vid behandling av personuppgifter. De författningar som är vanligast förekommande i Försvarsmaktens verksamhet är följande författningar.

- Personuppgiftslagen (1998:204), PuL.
- Personuppgiftsförordningen (1998:1191), PuF.
- Lagen (2007:258) om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst, PuL UNDSÄK.
- Förordningen (2007:260) om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst, PuF UNDSÄK.

Datainspektionen (DI) har givit ut allmänna råd, *Säkerhet för personuppgifter*. I de allmänna råden finns exempel på administrativa och tekniska säkerhetsåtgärder som PuL ställer på informationssäkerhet när man behandlar personuppgifter, d.v.s. upplysningar som kan knytas till enskilda personer i livet.

[1] Tidigare kallades denna analys för *författningsanalys.*



Postadress: Högkvarteret, 107 85 Stockholm
Besöksadress: Lidingövägen 24
Telefon: 08-788 75 00
Telefax: 08-788 77 78
E-post, Internet: exp-hkv@mil.se
www.forsvarsmakten.se/hkv

Försvarsmakten har i ett antal skrivelser[2] förtydligat vilka krav som gäller för IT-system som behandlar personuppgifter.

MUST har i samverkan med personuppgiftsombudet på juridiska staben i Högkvarteret, sammanställt de krav som gäller för ett IT-system som behandlar personuppgifter. Kraven ska inarbetas i underbilaga 1:2, IT-systemets säkerhetsspecifikation (ITSS), som *tillkommande funktionella krav.* i Beslut om krav på godkända säkerhetsfunktioner version 3.0 (KSF v3.0) 2012-09-24 10 750:64354.

**Känsliga personuppgifter eller övriga personuppgifter**

För att kunna bestämma vilka krav som ett IT-system ska uppfylla måste det klarläggas om det rör sig om känsliga personuppgifter eller inte. Om känsliga personuppgifter behandlas, ställs normalt sett högre krav på säkerheten.

Som känsliga personuppgifter betecknas enligt lagstiftningen uppgifter som avslöjar:
- ras eller etniskt ursprung,
- politiska åsikter,
- religiös eller filosofisk övertygelse,
- medlemskap i fackförening.

Vidare omfattas personuppgifter som rör hälsa eller sexualliv. Som exempel på uppgifter som normalt sett klassas som känsliga personuppgifter kan nämnas.
- Sjuklön och rehabilitering av arbetstagare.
- Uppgift om allergi.
- Handikapp, ex. handikappanpassning och ersättning.
- När personal inom Försvarsmakten inför en internationell militär insats besöker en sjukvårdsinrättning för att få vaccinationer.
- Forskningsprojekt som har till syfte att följa upp personalhälsan hos de som har deltagit i en internationell militär insats.

En annan kategori personuppgifter som regelmässigt har högre behov av skydd, är lagöverträdelser. Dessa innefattar uppgifter om brott (t.ex. brottsmisstankar), domar i brottmål, straffprocessuella tvångsmedel eller administrativa frihetsberövanden. Lagöverträdelse klassificeras inte som känsliga enligt PuL men jämställs oftast med känsliga uppgifter när det gäller kraven på säkerhet.

De finns andra typer av personuppgifter som typiskt sett är mer skyddsvärda än normalfallet. Dessa uppgifter behöver inte vara känsliga enligt lag eller ens omfattas av sekretess. I korthet rör det uppgifter som den registrerade inte sprider allmänt. Uppgifter som typiskt sett är av denna karaktär, rör t.ex. problem inom

[2] Se fotnot 3 och 4

familjen eller på arbetet. Det kan även röra uppgifter av privat ”dagbokskaraktär”. En annan typ av skyddsvärda uppgifter, är kontokortuppgifter vilka får anses ömtåligare av andra skäl än rena integritetsskäl. Som exempel på sådana personuppgifter är följande:

- Enskilds personliga och ekonomiska förhållanden inom bank- och försäkringsväsendet,
- uppgifter inom kreditupplysning eller inkassoverksamhet.

Ytterligare en annan typ av skyddsvärda uppgifter, av andra skäl än rena integritetsskäl är uppgifter om vapeninnehav.

*Som exempel på personuppgifter som normalt inte är att anse som känsliga personuppgifter som följer av:*
- *medlemskap*
- *anställningsförhållande,*
- *kundförhållande eller*
- *något därmed jämförligt förhållande.*

Personnummer är en kategori som inte sällan upplevs känsligare av folk i allmänhet. De är inte känsliga per definition i PuL och kan vara motiverade att hantera, t.ex. som identitetsbärare mellan IT-system. Personnumren ska dock i normalfallet skyddas så att de enbart exponeras för de som behöver uppgifterna i sin befattning.

## Säkerhetskrav på IT-system

Vid utveckling av ett IT-system, ska systemets godkända säkerhetsfunktioner vara anpassade för behandling av personuppgifter.

Utöver alla händelser som är av betydelse för säkerheten i systemet ska även händelser avseende personuppgifter registreras i säkerhetsloggen.

### Krav på IT-system som behandlar känsliga personuppgifter

Funktionella säkerhetskrav enligt underbilaga 1:3 till KSF v3.0

- SFBK_AUT uppfyller DI krav ifall U (Utökad) tillämpas (SFBK_AUT.1-15).
- SFSL_REG uppfyller DI krav ifall U (Utökad) tillämpas (SFSL_REG.1-5).
- Övriga funktionella säkerhetskrav ska vara lägst G (Grund).

Om känsliga personuppgifter ska kommuniceras till och från Försvarsmakten över sådana nätverk som går utanför FM IP-nätet ska kraven i skrivelsen[3], *Kryptering av känsliga personuppgifter* följas.

[3] HKV 2007-02-19 bet. 20 400:63221 Kryptering av känsliga personuppgifter

Om känsliga personuppgifter ska publiceras på intranätet eller i ett gemensamt nätverk ska skrivelsen[4], *Beslut angående hantering av personuppgifter i samband med diarieföring och skanning av handlingar* följas.

**Krav på IT-system som behandlar övriga personuppgifter**

Funktionella säkerhetskrav enligt underbilaga 1:3 till KSF v3.0

- SFSL_REG uppfyller DI krav ifall U (Utökad) tillämpas (SFSL_REG.1-5).
- Övriga funktionella säkerhetskrav ska vara lägst G (Grund).

Om övriga personuppgifter ska publiceras på intranätet eller i ett gemensamt nätverk ska skrivelsen[4], *Beslut angående hantering av personuppgifter i samband med diarieföring och skanning av handlingar* följas.

**Rekommendationer utöver KSF**

Nedan återfinns några exempel på rekommendationer som framförallt är hämtade från Datainspektionens allmänna råd, *Säkerhet för personuppgifter*.[5] Rekommendationerna gäller oavsett om IT-systemet behandlar känsliga personuppgifter eller övriga personuppgifter.

- IT-system som används för behandling av personuppgifter bör ha ett tillfredsställande skydd mot stöld och händelser som kan förstöra utrustningen.
- Rutiner för användning av portabla IT-system och regler vid distansarbete bör upprättas och vara anpassade avseende känsligheten på den personuppgiftsbehandling som ska genomföras.
- För att säkerställa att endast behörig personal får tillträde till utrymmen där IT-system finns, bör rutiner för tillträdeskontroll upprättas.
- För att förhindra förlust av personuppgifter bör rutiner för säkerhetskopiering finnas. Av en säkerhetsmålsättning för ett IT-system bör det framgå vilken säkerhetskopiering ett IT-system behöver och vilka åtgärder som måste vidtas för att säkerhetskopieringen ska få avsedd effekt.
- När lagringsmedier som innehåller personuppgifter inte längre ska användas för sitt ändamål bör lagringsmedierna förstöras, eller alternativt raderas på sådant sätt att personuppgifterna inte kan återskapas. Innan en förstöring eller radering av personuppgifterna genomförs måste Riksarkivets föreskrifter och allmänna råd beaktas. Vidare måste det säkerställas att Riksarkivet inte har fattat beslut om att personuppgifterna ska bevaras. Innan en förstöring eller radering bör kontakt alltid tas med en arkivarie, och om personuppgifterna finns vid MUST, MUST arkivarie. Vid behandling av personuppgifter enligt

[4] HKV 2006-01-25 bet. 20 400:61549 Beslut angående hantering av personuppgifter i samband med diarieföring och skanning av handlingar
[5] Reviderad i december 2008.

PuL UNDSÄK finns särskilda gallringsbestämmelser såväl i PuL UNDSÄK som i PuF UNDSÄK.

– Reparation och service bör ske på ett sådant sätt att personuppgifter inte blir tillgängliga för obehöriga. Ett personuppgiftsbiträdesavtal måste träffas med serviceföretag. Ett sådant avtal bör till exempel innehålla bestämmelser om vilka säkerhetsrutiner som ska tillämpas i samband med service. För att få tillgång till mallar som avser personuppgiftsbiträdesavtal kan kontakt tas med Försvarsmaktens personuppgiftsombud vid den juridiska staben i Högkvarteret.

Ytterligare åtgärder som inte nämns här kan vara nödvändiga för att skydda personuppgifterna som behandlas. Dessa åtgärder ska då vara identifierade genom den säkerhetsanalys[6] som ska göras för IT-systemet.

**Beredning av ärendet**

I beredningen av ärendet har även örlkn Christer Skagert (C MUST SÄKK SÄKT Ark) och övlt Patrik Lind (C MUST SÄKK SÄKS) deltagit.

**Beslut**

Dessa säkerhetskrav har beslutats av överste Mattias Hanson I den slutliga handläggningen har avdelningsdirektör Zenobia Rosander, försvarsjurist Anders Wiklund, och som föredragande kapten Stefan Styrenius.

Mattias Hanson
C MUST SÄKK

Stefan Styrenius

[6] Se H SÄK Grunder

**Sändlista**
HKV
LG, I 19, K 3, P 4, P 7, A 9, Lv 6, Ing 2, LedR, TrängR,
1. ubflj, 3. sjöstriflj, 4. sjöstriflj, Amf 1, MarinB,
F 7, F 17, F 21, Hkpflj,
FMLOG, FMTM, SOG,
MHS K, MHS H, MSS, SSS, LSS, HvSS, FMTS, SWEDEC, SkyddC,
FMUndSäkC,
FM HRC, FömedC

Som ori
FMV

Inom HKV
LEDS CIO
LEDS PRIO
PROD LEDUND
MUST
MUST SÄKK (avsett för Christer Skagert)
JURS