2017-04-28 /Nicu

1

FRA

REDOGÖRELSE

A61

2017-04-27

FRA beteckning
20 400:3383/17:1

DATAINSPEKTIONEN
Ink. 2017 -04- 28
Dnr. Ag. 191 1002-2017 Hk.

Datainspektionen
Box 8114
104 20 Stockholm

Er handläggare	Ert datum	Er beteckning
	2016-10-24	Dnr 2331-2015
FRA handläggare	FRA föreg. datum	FRA föreg. beteckning
Kári Ólafsson		

Redogörelse avseende regelbunden logguppföljning i försvarsunderrättelseverksamheten

Datainspektionen konstaterade i beslut den 24 oktober 2016 att Försvarets radioanstalt (FRA) genom att inte genomföra regelbundna logguppföljningar i försvarsunderrättelseverksamheten behandlar personuppgifter i strid med 3 kap. 2 § första stycket lagen (2007:259) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet (FRA-PUL).

FRA har förelagts att till Datainspektionen senast den 1 maj 2017 lämna en skriftlig redogörelse för de åtgärder som myndigheten har vidtagit och avser att vidta i fråga om den centrala logganalysfunktionen.

Nedan följer FRA:s skriftliga redogörelse.

Sammanfattning

FRA har under 2016 inlett uppbyggnaden av en central logganalysfunktion, Security Operation Center (SOC-funktion), och från den 1 januari 2018 kommer regelbunden logganalys av FRA:s it-system att inledas.

Under 2016 har utvecklingen av SOC-funktionens it-system för logganalys (analysmiljö) påbörjats. Logguppföljning har även testats i en utvecklings- och testmiljö. Sen-

FRA
Box 301
161 26 BROMMA

Telefon
08 - 471 46 00

Telefax

Org.nr
20 21 00 - 0365

FRA

ast juli 2017 kommer provdrift av analysmiljön att ske. Analysmiljön ska därefter ackrediteras under hösten 2017.

Interna föreskrifter och allmänna råd för uppföljning och kontroll av loggar ska beslutats efter samråd med Datainspektionen under 2017.

Uppföljning av loggar

Loggar sparas i de it-system som genererar dem. Det sker i dagsläget inte någon centraliserad analys av loggar. Det är berörd informationsägares ansvar att se till att logganalys sker. Efter påpekande från Datainspektionen 2010 började FRA med stickprovskontroller av loggar som genereras i it-system som används inom försvarsunderrättelse- och utvecklingsverksamheten.

Åtgärder som FRA har vidtagit i fråga om SOC-funktionen

2015
Under 2015 har det initiala planeringsarbetet med att inrätta en SOC-funktion på myndigheten för central logganalys på FRA påbörjats.

2016
FRA:s generaldirektör har den 29 september 2016 beslutat att inrätta en SOC-funktion för central logganalys på FRA. Enligt beslutet ska SOC-funktionens analysmiljö vara driftsatt senast den 1 januari 2018. Den som ansvarar för kontroll och uppföljning av loggar i FRA:s försvarsunderrättelse- och utvecklingsverksamhet kommer ha möjlighet att regelbundet kontrollera och följa upp loggar i försvarsunderrättelseverksamheten med hjälp av SOC-funktionen.

Det tekniska arbetet med att installera och driftsätta SOC-funktionens analysmiljö har påbörjats under senare delen av 2016. Logguppföljning från ett antal it-system som används i annan verksamhet än försvarsunderrättelseverksamheten har testats i en utvecklings- och testmiljö.

It-säkerhetsexperter har rekryterats till SOC-funktionen.

Fram till och med den 27 april 2017
Arbetet med utveckling och installation av SOC-funktionens analysmiljö har fortsatt under första delen av 2017. Samtliga servrar och den programvara, som ska ingå i analysmiljön, har installerats och initialt konfigurerats. De it-system som anslutits till ut-

FRA

vecklings- och testmiljön har anslutits till analysmiljön. It-system som används inom FRA:s försvarsunderrättelseverksamhet har börjat anslutas till analysmiljön.

Ytterligare medarbetare har rekryterats till FRA:s internkontroll. Internkontrollen ska, i samverkan med SOC-funktionen, genomföra regelbundna logguppföljningar i försvarsunderrättelse- och utvecklingsverksamheten.

Arbete med att upprätta interna föreskrifter och allmänna råd för uppföljning och kontroll av loggar som reglerar SOC-funktionens arbete pågår. Föreskrifterna ska vara färdigställda och beslutade av FRA:s generaldirektör innan analysmiljön tas i drift.

Åtgärder som FRA avser att vidta i fråga om SOC-funktionen

Efter den 27 april 2017
SOC-funktionens analysmiljö beräknas vara redo för provdrift i juli 2017. Under provdriften ska logguppföljning från it-system som används inom såväl FRA:s försvarsunderrättelseverksamhet som FRA:s övriga verksamhet testas.

FRA avser att i närtid begära samråd om föreskrifterna med Datainspektionen i enlighet med 13 § förordningen (2007:261) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet.

Under hösten 2017 ska SOC-funktionens analysmiljö ackrediteras. Under hösten ska även rutiner för uppföljning och kontroll samt rutiner för anslutning av it-system till SOC-funktionens analysmiljö färdigställas.

2018
Från och med den 1 januari 2018 beräknas regelbunden logganalys påbörjas av it-system som anslutits under provdriften. Övriga it-system kommer fortlöpande att anslutas till analysmiljön för regelbunden logganalys.

Det tar ca tre veckor att ansluta ett it-system till analysmiljön. It-system som används i försvarsunderrättelse- och utvecklingsverksamheten kommer prioriteras.

I detta ärende har generaldirektören Dag Hartelius beslutat. I den slutliga handläggningen har också deltagit chefsjuristen Michaela Dráb, tjf planeringschefen Petra Sävelin, stf avdelningschefen Anna Lalic Danielsson (Sigund), tjf avdelningscheferna Jim Nyberg (Cyber) och Eva Hallberg (avd V), säkerhetshandläggaren Katrin Tistam (avd V/Säk), samt juristen Kári Ólafsson (avd V/Rätts), tillika föredragande.

FRA

Försvarets radioanstalt

Dag Hartelius

Kári Ólafsson

Sändlista
För kännedom:
Försvarsdepartementet/Sund

Internt FRA
GD
ÖD
Chefsjuristen
C Plan
AC
C Säk (avd V)
KC Rätts (avd V)
Katrin Tistam (avd V)