



REMISSYTTRANDE

2022-11-23

FRA beteckning

Dnr 2.4.2:4100/22:2

Finansdepartementet
fi.remissvar@regeringskansliet.se
fi.fma.b@regeringskansliet.se

Er handläggare

Ert datum

Er beteckning

2022-09-02

Fi2022/02529

FRA handläggare

FRA föreg. datum

FRA föreg. beteckning

Jenny Forslund

Promemorian Ökad motståndskraft i betalningssystemet

Finansdepartementet har skickat promemorian Ökad motståndskraft i betalningssystemet på remiss. Försvarets radioanstalt (FRA) har granskat förslagen mot bakgrund av myndighetens uppdrag och om förslagen kan komma att påverka myndighetens verksamhet. FRA vill därför lämna följande synpunkter på förslagen i promemorian. Synpunkterna följer promemorians disposition.

7.2 Riskhantering och 7.3 Beredskap

Digitaliseringen av betalningsmarknaden har pågått under en längre tid och har ökat de senaste åren. Digitala betalningar är idag betydligt vanligare än kontanta betalningar. De bolag som omfattas av förslagen hanterar ett mycket stort antal betalningar med ett flertal olika betalningssätt. Enligt promemorian innebär det att incidenter i verksamheten kan medföra en betydande störning för betalningssystemet i stort. Kortvariga störningar i betalningssystemet riskerar att få stora konsekvenser för samhället och längre avbrott kan dessutom innebära risk för störningar av den finansiella stabiliteten i stort.

Mot den bakgrunden är det avgörande att det finns en medvetenhet om de risker som kan uppstå och krav på att kunna återuppta verksamheten inom kort efter ett avbrott. FRA instämmer i förslagen och vill särskilt understryka de risker som cyberattacker, utförda av aktörer med direkt avsikt att skada eller störa verksamheten, kan föra med sig för bolagen och vikten av att även detta ses som en operativ risk som bolagen ska kunna hantera.

7.4 Informations-, it- och cybersäkerhet

Förslaget innebär krav på clearingbolag att ha strategier för informations-, it- och cybersäkerhet som identifierar, bedömer och hanterar risker, hot och sårbarheter. Syftet med förslaget är att säkerställa fullgod behörighetshantering till datasystem, incidenthantering, hantering och kvalitetssäkring av it- och systemförändringar och ett fullgott cyberskydd. Mot bakgrund av den ökade digitaliseringen av betalningssystemet och de berörda företagens stora roll i detta är kraven relevanta. FRA instämmer därför i förslaget.

7.6 Uppdragsavtal

Det är viktigt att de krav som föreslås när det gäller riskhantering, beredskap och cybersäkerhet får genomslag också i fall när ett clearingbolag utkontrakterar verksamhet till uppdragstagare. FRA instämmer därför i förslaget om nya krav vid utkontraktering.

Allmänt om FRA

FRA är en civil myndighet under Försvarsdepartementet med ca 950 anställda. FRA är en del av svensk underrättelsetjänst med uppgift att bedriva försvarsunderrättelseverksamhet till stöd för svensk utrikes-, säkerhets- och försvarspolitik samt i övrigt för kartläggning av yttre hot mot landet enligt lagen (2000:130) om försvarsunderrättelseverksamhet. Inom försvarsunderrättelseverksamheten ska FRA bedriva signalspaning enligt lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet och till lagen anslutande förordning.

FRA bedriver signalspaning i syfte att kartlägga bl.a. yttre militära hot, internationell terrorism, allvarliga yttre hot mot samhällets infrastrukturer, främmande underrättelseverksamhet mot svenska intressen och övriga internationella företeelser som har betydelse för svensk utrikes-, säkerhets- och försvarspolitik. All signalspaning är riktad mot utländska förhållanden och sker på uppdrag av regeringen, Regeringskansliet, Försvarmakten, Säkerhetspolisen och Nationella operativa avdelningen inom Polismyndigheten. Uppdragsgivarna är fortlöpande i behov av underrättelserapportering och signalspaningsverksamheten bidrar kontinuerligt till att skydda Sverige och svenska intressen.

FRA

FRA bedriver även teknisk informationssäkerhetsverksamhet. FRA ska ha hög teknisk kompetens inom informationssäkerhetsområdet. FRA får efter begäran stödja sådana statliga myndigheter och enskilda verksamhetsutövare som hanterar information som bedöms vara känslig från sårbarhetssynpunkt eller i ett säkerhets- eller försvarspolitiskt hänseende. FRA ska särskilt kunna stödja insatser vid nationella kriser med it-inslag, medverka till identifiering av inblandade aktörer vid it-relaterade hot mot samhällsviktiga system, genomföra it-säkerhetsanalyser och ge annat tekniskt stöd.

FRA har även genom regeringsbeslut¹ fått uppdrag att, tillsammans med Försvarsmakten (FM), Myndigheten för samhällsskydd och beredskap (MSB) och Säkerhetspolisen, i nära samverkan med Försvarets materielverk (FMV), Post- och telestyrelsen (PTS) och Polismyndigheten, fördjupa samverkan inom cybersäkerhetsområdet genom ett nationellt cybersäkerhetscenter (NCSC).

Uppgifter rörande FRA:s verksamhet omfattas till stora delar av sekretess enligt 15 kap. 2 § offentlighets- och sekretesslagen (2009:400), OSL.

I detta ärende har chefsjuristen Michaela Dráb beslutat. I den slutliga handläggningen har också deltagit chefen för rättsenheten Per Fabricius samt juristen Jenny Forslund (C JUR:s kansli/Rätts), tillika föredragande.

Försvarets radioanstalt

Michaela Dráb

Jenny Forslund

¹ Uppdrag om fördjupad samverkan inom cybersäkerhetsområdet genom ett nationellt cybersäkerhetscenter, regeringsbeslut den 20 december 2020, Fö2019/01330.

FRASändlistaExternt för kännedom

Försvarsdepartementet/Sund

Försvarsdepartementet/Rättssekretariatet

Internt FRA

GD

ÖD

C JUR

Bitr. C JUR

C GD:s stab

C KOM

AC

C Rätts