RIKSGÄLDS KONTORET
THE SWEDISH NATIONAL DEBT OFFICE

REMISSVAR
2004-04-27 DNR 2004/770

Försvarsdepartementet
103 33 STOCKHOLM

PM med förslag till ny sekretessbestämmelse avseende risk- och sårbarhetsanalyser

(Dnr Fö2004/661/RS)

Riksgäldskontoret anser att det är angeläget att det införs sekretess för de risk- och sårbarhetsanalyser som myndigheterna är skyldiga att genomföra enligt förordningen (2002:472) om åtgärder för fredstida krishantering och höjd beredskap.

Emellertid bör sekretess gälla inte bara för de risk- och sårbarhetsanalyser som myndigheterna är skyldiga att genomföra enligt denna förordning, som avser beredskapsplanering för totalförsvaret, utan även i övrigt för utredningar som myndigheter företar avseende risken för intrång i myndighetens lokaler och IT-system. Sådana riskbedömningar kan myndigheter vilja genomföra på eget initiativ vid sidan av de analyser som föreskrivs i förordningen. För Riksgäldskontorets del finns det behov av att – utöver totalförsvarsberedskapen - se till att det finns ett väl fungerande säkerhetsskydd för våra lokaler och IT-system eftersom vi hanterar mycket stora belopp i vår verksamhet. Myndigheternas interna utredningar av risker för intrång i lokaler och IT-system bör därför generellt omfattas av sekretess. Om sådana utredningar är offentliga riskerar man att myndigheternas säkerhetsskydd blir mindre effektivt.

I företag och myndigheter, vilka liksom Riksgäldskontoret har hand om stora ekonomiska värden, är det väsentligt att hantera de operativa riskerna i verksamheten. Denna riskhantering består typiskt sett av fyra moment: (1) riskidentifiering, (2) riskutvärdering, vilket innebär bedömning av sannolikheten för och konsekvenser av olika identifierade risker, (3) riskhantering, vilket innebär att man kontrollerar, begränsar och åtgärdar identifierade risker samt (4) riskövervakning, vilket innebär regelbunden rapportering av risker och riskexponering. Om de handlingar som uppstår vid hanteringen av de operationella riskerna i verksamheten är offentliga hos myndigheten kan själva förekomsten av dessa handlingar utgöra en operativ risk hos myndigheten vilket är en olycklig konsekvens av arbetet med att förbättra säkerheten i verksamheten. Vidare kan offentligheten in-

POSTADRESS/POSTAL ADDRESS SE-103 71 Stockholm Sweden
BESÖK/VISITORS Norrlandsgatan 15
TELEFON/TELEPHONE NAT. 08-613 15 00 INT. +46 8 613 15 00
TELEFAX NAT. 08-21 21 63 INT. +46 8 21 21 63
INTERNET MAIL rgk@rgk.se WEB WWW.rgk.se
ORG.NR. 202100-2635

nebära att myndigheterna kanske avstår från att kartlägga operationella risker. Det är därför av yttersta vikt att myndigheters interna åtgärder för att hantera operationella risker i verksamheten skyddas av sekretess.

Vi noterar att förslaget i prop 2003/94:93 om ändring i 5 kap 2 § sekretesslagen innebär en utvidgning av sekretessen för säkerhets- eller bevakningsåtgärder för IT-system i jämförelse med vad som gällt hittills. Detta förslag omfattar dock inte utredningar av risker för intrång i IT-system utan bara genomförda säkerhets- eller bevakningsåtgärder. Även utredningar och bedömningar av riskerna för intrång bör enligt vår mening som ovan anförts omfattas av sekretess. Vi anser inte att det finns något väsentligt offentlighetsintresse som uppväger behovet av ett sådant utvidgat sekretesskydd.

Vi anser därför att den föreslagna nya bestämmelsen i 5 kap 8 § sekretesslagen bör få följande lydelse.

> Sekretess gäller för uppgift som hänför sig till myndighetens verksamhet som avser *utredning och bedömning av risk för intrång i myndighetens lokaler eller i myndighetens system för automatiserad behandling av information*, risk- och sårbarhetsanalyser eller planering och förberedelser för hantering av fredstida krissituationer, om det kan antas att syftet med verksamheten motverkas om uppgiften röjs.

I detta ärende har chefsjuristen Anne Gynnerstedt beslutat. Övriga närvarande har varit säkerhetschefen Britt-Marie Palm och avdelningsdirektören Arvid Hessén, föredragande.

Anne Gynnerstedt Arvid Hessén