Regel

BESLUTSDATUM:	2014-12-17
BESLUT AV:	Anders Vredin
BEFATTNING:	Avdelningschef
ANSVARIG AVDELNING:	Stabsavdelningen
FÖRVALTNINGSANSVARIG:	Lars Andersson
HANTERINGSKLASS	Ö P P E N
Senast granskad:	2018-02-02

SVERIGES RIKSBANK
SE-103 37 Stockholm
(Brunkebergstorg 11)

Tel +46 8 787 00 00
Fax +46 8 21 05 31
registratorn@riksbank.se
www.riksbank.se

DNR 2014-768-STA

Klassificering och hantering av Riksbankens information

Riksbanken hanterar information som, om obehöriga får åtkomst till den, kan innebära skada för Riksbanken och dess medarbetare, kunder eller samarbetspartners. För att begränsa riskerna vid hantering av information, finns denna regel som anger hur Riksbankens information ska klassificeras, märkas och hanteras med hänsyn till informationens konfidentialitet.

Med "information" avses alla typer av information oberoende av hur den lagras eller kommuniceras, till exempel dokument på papper, elektroniskt lagrad information, e-post, telefonsamtal och faxmeddelanden. Med konfidentialitet avses behovet av att skydda information från att obehöriga tar del av den.

Riksbankens information ska:

- *klassificeras* utifrån hur allvarliga konsekvenserna kan bli om den sprids till obehöriga och i tillämpliga fall *märkas* utifrån beslutad hanteringsklass,
- *hanteras* på ett sätt som överensstämmer med klassificeringen.

Eftersom Riksbanken omfattas av lagstiftning som berör hantering av information[1] beskriver regeln även hur Riksbankens klassificering och hantering av information förhåller sig till denna lagstiftning.

Regeln riktar sig till alla anställda i Riksbanken och till uppdragstagare som för Riksbankens räkning får ta del av Riksbankens information. Vid tveksamhet kring tolkningen av dessa regler ska riskenheten på stabsavdelningen kontaktas.

Ansvar

Det är varje avdelningschefs ansvar att se till att medarbetarna får den information och utbildning de behöver för att kunna följa dessa regler.

Den som skapar information, tar emot information från externa parter, eller på annat sätt ansvarar för hanteringen av information, ska klassificera och märka informationen med rätt hanteringsklass. Klassificeringen ska utgå från vilka konsekvenser som kan uppstå om informationen sprids.

[1] Offentlighets- och sekretesslagen (2009:400) och lagen (2006:128) om säkerhetsskydd för Riksdagen och dess myndigheter.

Vid oklarheter ska närmaste chef eller riskenheten på stabsavdelningen tillfrågas.

Hanteringsklasser

Hanteringsklasserna utgår från vilka konsekvenser som kan uppstå om informationen sprids till obehöriga.[2]

Följande fyra hanteringsklasser ska användas för att klassificera information:

- ÖPPEN
- BEGRÄNSAD
- KÄNSLIG
- MYCKET KÄNSLIG

På engelska benämns Riksbankens hanteringsklasser RB PUBLIC (öppen), RB RESTRICTED (begränsad), RB CONFIDENTIAL (känslig) och RB STRICTLY CONFIDENTIAL (mycket känslig). Prefixet RB används för att undvika förväxling med externa parters hanteringsklasser, exempelvis ECB och IMF.

Hanteringsklass: ÖPPEN

Med ÖPPEN information avses information som antingen är avsedd för allmän spridning eller där konsekvensen vid spridning är **ingen** eller **obetydlig.**

Hanteringsklass: BEGRÄNSAD

Med BEGRÄNSAD information avses information som, om den kommer till obehörigas kännedom, innebär **liten** konsekvens för Riksbanken eller enskild juridisk eller fysisk person eller för något annat skyddsvärt intresse. Informationen är i första hand avsedd för Riksbankens medarbetare och kan spridas internt och är inte *avsedd* för extern spridning.

Hanteringsklass: KÄNSLIG

Med KÄNSLIG information avses information som, om den kommer till obehörigas kännedom, innebär **märkbara** konsekvenser för Riksbanken eller enskild juridisk eller fysisk person eller för något annat skyddsvärt intresse. Informationen ska ges **begränsad** spridning.

Hanteringsklass: MYCKET KÄNSLIG

Med MYCKET KÄNSLIG information avses information som, om den kommer till obehörigas kännedom, innebär **allvarliga** eller **mycket allvarliga** konsekvenser för Riksbanken eller enskild juridisk eller fysisk person eller för något annat skyddsvärt intresse. Informationen ska ges **mycket begränsad** spridning.

[2] Konsekvensnivåerna definieras närmare i Riksbankens regel för operativ risk.

Säkerhetsskyddad information

På Riksbanken hanteras även information som bedöms vara av vikt för rikets säkerhet och skyddet mot terrorism, i enlighet med lagen (2006:128) om säkerhetsskydd för Riksdagen och dess myndigheter. Detta rör dock endast en begränsad mängd information, till exempel information om skydd gällande kontanthanteringen.[3] Vid hanteringen av säkerhetsskyddad information kan det finnas behov av ytterligare säkerhetsåtgärder *utöver* de som gäller för MYCKET KÄNSLIG information. Säkerhetsskyddad information ska därför klassificeras och märkas som HEMLIG. Riksbankens säkerhetsskyddschef[4] ansvarar för att vid behov fastställa särskilda rutiner för hantering av säkerhetsskyddad information och att informera berörd personal om dessa.

Offentlighet och sekretess

Enligt offentlighets- och sekretesslagen (2009:400) har allmänheten och massmedierna rätt att ta del av allmänna handlingar hos statliga myndigheter, vilket innefattar Riksbanken. En handling är allmän om den förvaras hos en myndighet och är att anse som inkommen till eller upprättad hos myndigheten. Däremot är arbetshandlingar, utkast, minnesanteckningar, muntlig information och liknande normalt inte att betrakta som allmänna handlingar. När en handling begärs ut ska Riksbanken göra en prövning av om den kan lämnas ut i enlighet med gällande lagstiftning. Hanteringsklassen kan indikera om informationen kan lämnas ut direkt, eller om en prövning bör göras, men oavsett hur Riksbanken valt att klassificera informationen kan den behöva lämnas ut.[5]

Om det kan antas att en uppgift i en allmän handling omfattas av sekretess, kan en sekretessmarkering göras på handlingen. En sådan markering kan göras i form av en ruta med texten "Sekretess", en hänvisning till tillämplig sekretessbestämmelse samt datum då markeringen gjordes. Om sekretessmarkering görs måste handlingen alltid diarieföras.

Utbyte av information med externa parter

Klassificering av inkommande information

När information kommer in från andra myndigheter, företag, ECB, IMF, BIS osv. är det Riksbankens hanteringsregler som avgör vilken hanteringsklass som ska tillämpas i Riksbanken. Den klassificering som tillämpas av den som lämnar informationen till Riksbanken ska dock beaktas.

[3]Säkerhetsskyddet ska i första hand beakta konsekvenserna för *andra delar av samhället* om viss Riksbanksinformation förvanskas eller hamnar i orätta händer.
[4] Denna roll innehas av Riksbankens säkerhetschef
[5] Läs mer om offentlighet och sekretess och allmänna handlingar i Riksbankens "Information om offentlighet och sekretess" på Banonätet/Stöd och service/Diariet.

För information som är direkt relaterad till arbetet i ECB:s beslutande organ, ECBS-kommittéer eller undergrupper till dessa, eller ECBS-projekt, gäller särskilda regler.[6] Dessa uppfylls förutsatt att inkommande ECBS-information hanteras enligt följande:

- **ECB Restricted** hanteras som **Begränsad** information
- **ECB Confidential** hanteras som **Känslig** information
- **ECB Secret** hanteras som **Mycket Känslig** information.

ECBS-information enligt ovan som skapas i Riksbankens verksamhet behöver märkas med aktuell ECB hanteringsklass endast om den ska distribueras till andra aktörer inom ECBS.

Spridning av information till externa parter

En del av den information som skapas eller kommer in till Riksbanken delges även externa parter inom ramen för olika samarbeten. Eftersom Riksbanken inte kan styra fullt ut hur de externa parterna hanterar informationen ska hanteringsklassen tydligt framgå vid sådant informationsutbyte. Om informationen är "känslig" eller "mycket känslig" ska avtal eller annan överenskommelse finnas med den externa parten avseende hur informationen ska hanteras.

Klassificering

Kravet på klassificering gäller från det att informationen skapas eller kommer in till Riksbanken och så länge den existerar. Klassificeringen kan behöva förändras under den tid informationen finns i Riksbanken, eftersom informationens konfidentialitet kan ändras över tiden.

För att uppnå en enhetlig och konsekvent klassificering av Riksbankens information, ska informationshanteringsplaner finnas för Riksbankens olika processer. Planerna anger även vilken information som ska diarieföras och arkiveras.

För information som lagras och hanteras i IT-system ska en kritikalitetsbedömning genomföras för att fastställa hur informationen ska klassificeras.[7]

När informationen är placerad i en hanteringsklass är skyddsnivån fastställd och därefter ska eventuella skyddsåtgärder vidtas. Av tabellen på sidan 6 framgår vilka principiella skyddsåtgärder som ska vidtas för respektive tillämpning och hanteringsklass.

Märkning

Informationen ska märkas med hanteringsklass i samband med att den skapas eller kommer in till Riksbanken. Märkningen visar hur informationen ska förvaras och i

[6] För är att skydda känslig ECBS-information mot obehörig tillgång och obehörigt utlämnande har ECB-rådet beslutat att "ESCB Common rules and minimum standards for the handling of sensitive ESCB information" ska tillämpas även av centralbanker som ingår i ECBS men inte i Eurosystemet. Varje centralbank inom ECBS är ansvarig för att lämpliga åtgärder vidtas för att uppfylla dessa allmänna bestämmelser.

[7] Se Riksbankens regel för operativa risker.

övrigt hanteras och ska anges väl synligt. Syftet är att göra alla användare uppmärksamma på hur informationen ska hanteras. Där det är uppenbart opraktiskt eller av andra skäl inte möjligt behöver inte informationen märkas, men hanteringsklassen bör då framgå på annat sätt.

Öppen information behöver inte märkas om det är uppenbart att den är avsedd för allmän spridning, exempelvis trycksaker om Riksbanken och Riksbankens verksamhet.

Vid extern distribution eller vid delning av arbetsmaterial ska märkningen av "känslig" och "mycket känslig" information kvarstå, för att göra det tydligt för mottagaren att Riksbanken vill att informationen hanteras med försiktighet.

Omprövning av klassificering

För att informationen ska ha rätt skyddsnivå över tid kan klassificeringen behöva omprövas under informationens livslängd. Omprövningen bör göras av den som initialt klassificerat informationen.

Ett exempel är en rapport som förändras från "känslig" till "mycket känslig" under arbetets gång, för att sedan bli "öppen" i och med att den offentliggörs. En omprövning kan också behöva göras när information kompletteras med känsliga uppgifter eller om ett rent faktamaterial kompletteras med bedömningar och slutsatser.

Information som kommer att publiceras och där upprättaren vet tidpunkten kan märkas med båda hanteringsklasserna enligt följande:

MYCKET KÄNSLIG t.o.m. 20YY-MM-DD, TT:MM, därefter ÖPPEN

Undantag

Avdelningschef får, inom sitt ansvarsområde enligt instruktionen, besluta om undantag från de skyddsåtgärder som anges i denna regel i tabellen på sidan 6. Beslutet ska dokumenteras och riskchefen ska informeras.

Ett undantag får beslutas om det av tekniska skäl, eller av skäl som Riksbanken inte rår över, inte är möjligt att upprätthålla en viss skyddsåtgärd. Undantaget ska avse viss särskilt angiven skyddsåtgärd och gälla under viss angiven tid. Undantaget får beslutas bara om det behövs för att arbetet ska kunna bedrivas effektivt och hänsyn måste tas till vilka konsekvenser som kan uppstå om obehöriga tar del av informationen.

Hantering

I tabellen nedan anges vilka skyddsåtgärder som gäller för respektive tillämpning och hanteringsklass. All information som hanteras i Riksbankens IT-miljö och lokaler omfattas av det grundskydd som finns i form av exempelvis inloggning och inpasseringskontroll. För information med högre hanteringsklass gäller sedan succesivt högre krav i de olika tillämpningarna. Tabellen är styrande för hanteringen, men för att underlätta det praktiska dagliga arbetet finns även en lathund, se Bil. 1.

För *elektronisk information* finns restriktioner när det gäller behörigheter, bearbetning, lagring, kommunikation och destruktion av information. Med *elektronisk information* avses datafiler, databaser, fax, video och annan strömmande media, fast och mobil telefoni etc.

För *pappersbaserad information* finns restriktioner när det gäller behörigheter, förvaring, distribution och destruktion. Med *pappersbaserad information* avses utskrivna dokument, anteckningar, trycksaker etc.

För *talad information* finns restriktioner när det gäller var och hur samtal ska föras.

	Öppen	**Begränsad**	**Känslig**	**Mycket Känslig**
Konsekvens vid spridning till obehöriga	Ingen eller Obetydlig	Liten	Märkbar	Allvarlig eller Mycket Allvarlig
Behörig att ta del av information	Inga restriktioner	Medarbetare på Riksbanken[8]	Den som har behov av informationen i sitt jobb eller kan komma att ha nytta av den. Tilldelas normalt på enhets- eller projektnivå	Den som har ett mycket starkt behov av informationen i sitt jobb. Tilldelas på individnivå
Spridning av information externt	Inga restriktioner	Efter bedömning att Riksbanken har nytta av spridning eller att det finns ett åtagande till motparten.	Spridning ska ske restriktivt. Avtal eller annan överenskommelse med motparten ska finnas	Spridning ska ske mycket restriktivt. Avtal med motparten ska finnas
Hantering av elektronisk information				
Bearbetning	Inga restriktioner	Inga restriktioner	På främmande utrustning med viss försiktighet[9]	Endast på Riksbanksutrustning
Lagring internt (i RB lokaler eller motsvarande)[10]	Inga restriktioner	På Riksbanksutrustning	På Riksbanksutrustning, i låsta utrymmen eller krypterat	På Riksbanksutrustning, krypteras
Lagring externt (utanför RB lokaler)	Inga restriktioner	På främmande utrustning med viss försiktighet[9]	På Riksbanksutrustning (krypterat) eller med 3e-partsavtal	På Riksbanksutrustning, krypteras. Utrustningen förvaras under uppsikt eller inlåst.

[8] Med medarbetare avses anställda och uppdragstagare med regelbundna eller längre uppdrag på Riksbanken. Förutsättningen är att personen har ett inloggningsID till Riksbankens IT-miljö.
[9] Exempelvis på en hemdator eller privat telefon, undvik användning av helt främmande utrustning
[10] Lagring i IT-system, PC, flyttbara datamedia etc. Med Riksbankens lokaler kan också menas avgränsade och godkända lokaler hos extern part.

	Öppen	Begränsad	Känslig	Mycket Känslig
Datakommunikation internt (i RB lokaler och nätverk)[11]	Inga restriktioner	Inga restriktioner	Krypteras om åtkomlig i publika utrymmen	Krypteras
Datakommunikation externt (utanför RB lokaler eller utanför RB nätverk)[12]	Inga restriktioner	Inga restriktioner	Krypteras	Krypteras
Återanvändning av datamedia	Inga restriktioner	Inga restriktioner	Efter radering med av Riksbanken godkänd teknik	Efter radering med av Riksbanken godkänd teknik
Destruktion[13]	Inga särskilda krav	Överskrivning	Radering med av Riksbanken godkänd teknik eller fysisk destruktion	Fysisk destruktion
Hantering av tryckt eller skriven information				
Förvaring internt (i RB lokaler) eller motsvarande[14]	Inga restriktioner	Inga restriktioner	I låst rum, låst skrivbordshurts eller motsvarande eller under uppsikt	I godkänt säkerhetsskåp eller under uppsikt
Förvaring externt (utanför RB lokaler)	Inga restriktioner	Under uppsikt eller i privata utrymmen	Under uppsikt eller dolt i privata utrymmen	I godkänt säkerhetsskåp eller under uppsikt
Distribution internt	Inga restriktioner	Inga restriktioner	Igenklistrat kuvert med internpost	Personligen eller budat i säkerhetskuvert
Distribution externt	Inga restriktioner	Igenklistrat kuvert eller motsvarande	Rekommenderat brev eller motsvarande	Säkerhetskuvert och av Riksbanken godkänt bud
Destruktion[13]	Inga restriktioner	Pappersåtervinning	Låst pappersåtervinning	Dokumentförstörare
Hantering av talad information				
I Riksbankens lokaler	Inga restriktioner	Inga restriktioner	Iaktta vaksamhet	I avskildhet[15]
Utanför Riksbankens lokaler	Inga restriktioner	Iaktta vaksamhet	I avskildhet	Bör undvikas

[11] Kommunikationen sker alltså innanför vårt fysiska (fastigheter) och vårt logiska (brandväggar) skalskydd.
[12] Kommunikation kan vara extern även om den sker i våra lokaler, om den sker utanför vårt logiska skalskydd.
[13] Destruktion av allmänna handlingar kräver gallringsbeslut
[14] Med Riksbankens lokaler kan också menas avgränsade och godkända lokaler hos extern part.
[15] Beakta risken för avlyssning när man är i avskildhet. Mobiltelefoner och annan utrustning med mikrofoner kan medvetet eller omedvetet fungera som inspelningsutrustning. Utrustning med mikrofoner kan antingen lämnas utanför eller, till exempel, i en bruslåda.

Bilaga 1: Lathund för hantering av Riksbankens information

	ÖPPEN	BEGRÄNSAD	KÄNSLIG	MYCKET KÄNSLIG
Internt elektroniskt lagrad information	Inga restriktioner	Åtkomst för Riksbankens medarbetare	Åtkomst genom begränsad behörighetstilldelning	Ska krypteras (ej lagring i DHS)
Extern datakommunikation	Inga restriktioner	Inga restriktioner	Ska krypteras	Ska krypteras
E-post internt	Inga restriktioner	Inga restriktioner	Märkning ska framgå i ämnesraden	Märkning ska framgå i ämnesraden, ska krypteras med bankens lösning för e-post
E-post externt	Inga restriktioner	Inga restriktioner	Ska krypteras med bankens lösning för e-post	Ska krypteras med bankens lösning för e-post
Handdator och mobiltelefoner	Riksbanksutrustning ska vara under uppsikt eller inlåst. Annars inga restriktioner	Riksbanksutrustning ska vara under uppsikt eller inlåst. Bör krypteras	Endast på Riksbanksutrustning. Informationen ska krypteras, utrustningen ska vara under uppsikt eller inlåst.	Endast på Riksbanksutrustning. Informationen ska krypteras, utrustningen ska vara under uppsikt eller inlåst. Chefs godkännande krävs
På hemdator	Inga restriktioner	Inga restriktioner	Information får bearbetas men ej lagras	Ej tillåtet
På främmande dator (ex.vis internetcafé)	Inga restriktioner	Inga restriktioner	Bör undvikas	Ej tillåtet
PC internt	Inga restriktioner	Inga restriktioner	Hårddisken ska krypteras	Hårddisk samt berörda filer ska krypteras
PC på resan	Under uppsikt eller i låst rum.	Under uppsikt eller i låst rum.	Under uppsikt eller i låst rum, hårddisken ska krypteras	Under uppsikt eller i låst rum, hårddisk samt berörda filer ska krypteras. Chefs godkännande krävs.
USB-minne, CD-skivor, disketter etc.	Inga restriktioner	Bör krypteras	Informationen ska krypteras, minnet ska förvaras under uppsikt eller inlåst.	Informationen ska krypteras, minnet ska förvaras under uppsikt eller inlåst. Chefs godkännande krävs.

	ÖPPEN	BEGRÄNSAD	KÄNSLIG	MYCKET KÄNSLIG
Utskrift	Inga restriktioner	Inga restriktioner	Ska skrivas ut på nätverksskrivare med kort-identifiering, alternativt lokal skrivare	Ska skrivas ut på krypterad nätverksskrivare med kort-identifiering, alternativt lokal skrivare
Telefonsamtal externt	Inga restriktioner	Inga restriktioner	Samtal ska föras avskilt och under försiktighet	Bör undvikas
Fax	Inga restriktioner	Inga restriktioner	Fax övervakas under sändning/ mottagning	Kryptofax ska användas
Makulering av IT-media, disk, CD, band, etc.	Inga restriktioner	Inga restriktioner	Överskrivning eller destruktion inom banken	Ska förstöras inom banken (destruktion)
Intern förvaring av pappersdokument	Inga restriktioner	Inga restriktioner	Under uppsikt eller dolt i arbetsrum, bör vara inlåst i skrivbord etc.	Under uppsikt eller inlåst i säkerhetsskåp
Förvaring av dokument i hemmet	Inga restriktioner	Inga restriktioner	Under uppsikt eller inlåst i skrivbord etc.	Under uppsikt eller inlåst i säkerhetsskåp. Chefs godkännande krävs.
Förvaring av dokument i parkerat fordon	Inga restriktioner	Bör undvikas	Inte tillåtet	Inte tillåtet
Dokument på resan	Inga restriktioner	Inga restriktioner	Under uppsikt eller inlåst i väska/safety box i låst rum.	Under uppsikt, eller inlåst i säkerhetsskåp. Chefs godkännande krävs.
Intern post	Inga restriktioner	Inga restriktioner	Personligen eller i igenklistrat kuvert	Personligen eller i dubbla kuvert och säkerhetstape
Extern post	Inga restriktioner	Igenklistrat kuvert	Ess-brev/rek	Dubbla kuvert, säkerhetstape och Ess-brev/rek
Makulering av dokument	Till pappersåter-vinning	Till pappersåter-vinning	Låst pappersåter-vinning (S-märkt)	Dokument-förstörare
Möten i Riksbankens lokaler	Inga restriktioner	Inga restriktioner	Iaktta vaksamhet, beakta risken för insyn i mötesrum.	Mötesorganisatör kan besluta att mobiltelefoner och annan utrustning med mikrofoner inte får medföras.