

FÖRSVARSMAKTEN



Handbok Sekretessbedömning Del A

2011

**Handbok för Försvarsmaktens
säkerhetstjänst, Sekretessbedömning Del A**

H Säk Sekrbed A



Handbok för Försvarmaktens säkerhetstjänst, Sekretessbedömning Del A (H Säk Sekrbed A), 2011 års utgåva (M7739-352028) fastställs för tillämpning fr.o.m. 2011-03-01.

Målgruppen är främst Försvarmaktens ledning, chefer för organisationsenheter, säkerhetschefer, IT-säkerhets- och signalskyddschefer samt annan personal som arbetar med informationssäkerhetsfrågor och med uppgifter som omfattas av sekretess. Handboken kan även vara intressant vid andra myndigheter än Försvarmakten som jämförelse och som orientering.

Juridiska staben vid Försvarmaktens högkvarter har ganskat handbokens innehåll avseende de rättsliga aspekterna.

Därmed upphävs

- Kapitel 1 och 20 samt bilagorna 1 och 2 i Handbok för Försvarmaktens Säkerhetsskyddstjänst, Sekretessbedömning (H SÄK Sekrbed), 1999 års utgåva (M7745-734081).
- Riktlinjer vid aggregation av uppgifter med avseende på informationssäkerhetsklasser (HKV 2006-05-05, 10 750:67663).
- Riktlinjer vid inplacering av hemliga uppgifter i informationssäkerhetsklass (HKV 2004-05-18, 10 440:68631).
- Bilaga 2 till Riktlinjer för klassificering av olika former av handlingar (HKV 2008-06-25, 10 812:72264).

Chefen för Säkerhetskontoret vid den militära underrättelse- och säkerhetstjänsten får fatta beslut om ändringar i handboken inom ramen för 2011 års utgåva.

Beslut i detta ärende har fattats av generalmajor Stefan Kristiansson. I den slutliga handläggningen har deltagit kontorschef John Daniels, överstelöjtnant Mattias Hanson, överstelöjtnant Mårten Wallén, Helena Rozi, Kim Hakkarainen, major Ola Areschoug samt, som föredragande, avdelningsdirektör Martin Waern.

Stefan Kristiansson

Chef för militära underrättelse- och säkerhetstjänsten

Martin Waern

© 2011 **Försvarmakten**, Stockholm

Att mångfaldiga innehållet i denna publikation, helt eller delvis, utan medgivande av Försvarmakten, är förbjudet enligt upphovsrättslagen.

Layout: Grafiska ateljén FMLOG APSA Grafisk produktion, Stockholm
M7739-352028 H Säk Sekrbed A

Central lagerhållning: Försvarets bok- och blankettförråd

Förord

Försvarmakten har liksom alla myndigheter en grundlagsreglerad skyldighet gentemot allmänheten att på begäran lämna ut allmänna handlingar. Samtidigt har myndigheten även en skyldighet att inte röja sådana uppgifter som omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400), nedan benämnd OSL.

Målgruppen för denna handbok är Försvarmaktens personal som i sitt arbete kommer i kontakt med uppgifter som omfattas av sekretess. Innehållet i handboken är av särskild betydelse för dem i vars arbete ingår att delta i handläggningen av ärenden som rör utlämnande av allmänna handlingar.

Nuvarande handbok för Försvarmaktens säkerhetsskyddstjänst sekretessbedömning (H SÄK Sekrbed) utkom 1999. Sedan 1999 har dock Försvarmaktens uppgifter och verksamhet förändrats på ett sådant sätt att den inte längre ger ett fullständigt stöd avseende bedömningen av om en uppgift omfattas av sekretess eller inte. 2004 skedde en förändring i Försvarmaktens regelverk avseende säkerhetsskydd och indelningen av hemliga uppgifter i fyra informationssäkerhetsklasser introducerades. Den 30 juni 2009 trädde OSL i kraft vilken då ersatte 1980 års sekretesslag. Den 1 mars 2010 trädde Försvarmaktens föreskrifter (FFS 2010:1) om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar i kraft.

Mot bakgrund av detta finns det ett behov av att komplettera stödet avseende såväl sekretessbedömning som placering av uppgifter i informationssäkerhetsklass. Denna handbok (Handbok för Försvarmaktens säkerhetstjänst sekretessbedömning del A) har som syfte att komplettera H SÄK Sekrbed 1999 avseende den teoretiska grunden för offentlighet och sekretess, ge en beskrivning av vissa sekretessbestämmelser, ge grunderna för placering av hemliga och utrikesklassificerade uppgifter i informationssäkerhetsklass samt beskriva arbetsgången vid utlämning av allmänna handlingar.

Handboken är uppbyggd på ett sådant sätt att inledningskapitlet beskriver grunden för informationsklassificering i Försvarmakten (kapitel 1) följt av en beskrivning av offentlighet och sekretess i det

allmännas verksamhet, för att ge en teoretisk grund för när uppgifter är offentliga eller omfattas av sekretess (kapitel 2).

Efter detta följer en beskrivning av fem utvalda sekretessbestämmelser som förekommer i Försvarmaktens verksamhet. Kapitlet är avsett att utgöra ett stöd för att bedöma om en uppgift är sekretess eller inte med stöd av i kapitlet beskrivna sekretessbestämmelser (kapitel 3). Kapitlet är inte uttömmande utan beskriver endast några allmänt förekommande sekretessbestämmelser i Försvarmaktens verksamhet.

Därefter ges en beskrivning av tillvägagångssättet för hur vissa uppgifter ska placeras i informationssäkerhetsklass. Detta gäller uppgifter som omfattas av sekretess och som rör rikets säkerhet (hemliga uppgifter¹) samt sådana uppgifter som omfattas av utrikessekretess, utan att röra rikets säkerhet, har åsatts en märkning som motsvarar en informationssäkerhetsklass – utrikesklassificerade uppgifter² (kapitel 4).

Slutligen beskrivs rutinerna vid ärenden som rör begäran om att få ta del av en allmän handling i Försvarmakten samt utlämnande av dessa (kapitel 5). I slutet på handboken finns bilagor med exempel på avslagsbeslut i ärenden om utlämnande av allmän handling, en förteckning över andra länders motsvarighet till informationsklasser samt råd om hur informationsklassificering kan formuleras.

I kommande skrivelser (del B) kommer det att ges en detaljerad beskrivning av informationsklassificeringen av uppgifter inom olika verksamhetsområden inom Försvarmakten.

Stefan Kristiansson

Chef för militära underrättelse- och säkerhetstjänsten

Innehåll

1 Informationsklassificering i Försvarmakten	9
1.1 Försvarmaktens informationstillgångar	9
1.2 Modell för informationsklassificering	9
1.3 Ansvar för informationsklassificeringen	11
1.4 Sammanfattning	11
2 Offentlighet och sekretess	13
2.1 Offentlighetsprincipen	13
2.1.1 Tryckfrihetsförordningen	14
2.1.2 En handling	14
2.1.3 Allmän handling	15
2.1.4 Arbetshandlingar	16
2.2 Sekretess	17
2.2.1 Beskrivning av sekretess	17
2.2.2 Bedömning av sekretess	18
2.2.3 Sekretessmarkering	19
2.2.4 Rätten att meddela och offentliggöra uppgifter	20
3 Beskrivning av sekretessbestämmelser	21
3.1 Inledning	21
3.2 Förvarssekretess	22
3.2.1 Tillämpning av förvarssekretess	22
3.2.2 Totalförsvaret	23
3.2.3 Förvarssekretess och rikets säkerhet	24
3.2.4 Sekretesstider	24
3.2.5 Rätten att meddela och offentliggöra uppgifter	24
3.2.6 Sammanfattning	25
3.3 Utrikessekretess	26
3.3.1 Tillämpning av utrikessekretess	26
3.3.2 Hantering av utländska uppgifter	27
3.3.3 Utrikessekretess och rikets säkerhet	28
3.3.4 Rätten att meddela och offentliggöra uppgifter	29
3.3.5 Sammanfattning	30
3.4 Säkerhets- och bevakningssekretess	30
3.4.1 Tillämpning av säkerhets- och bevakningssekretess	30
3.4.2 Byggnader, anläggningar, lokaler och inventarier	31
3.4.3 Telekommunikation och IT-system	32
3.4.4 Behörighet i IT-system	32
3.4.5 Rätten att meddela och offentliggöra uppgifter	33

3.5 Upphandlingssekretess	34
3.5.1 Tillämpning av upphandlingssekretes	34
3.5.2 Konsulter	35
3.5.3 Rätten att meddela och offentliggöra uppgifter	36
3.6 Affärssekretess	36
3.6.1 Tillämpning av affärssekretess	36
3.6.2 Sekretesstiden	37
3.6.3 Rätten att meddela och offentliggöra uppgifter	37
4 Informationssäkerhetsklasser	39
4.1 Inledning	39
4.2 Informationssäkerhetsklasser	39
4.3 Placering av hemliga uppgifter i informationssäkerhetsklass	43
4.3.1 Inledning	43
4.3.2 Förtida menbedömning	43
4.3.3 Informationssäkerhetsklassen HEMLIG/TOP SECRET	44
4.3.4 Aggregation	45
4.4 Placering av utrikesklassificerade uppgifter i informations- säkerhetsklass	47
4.4.1 Inledning	47
4.4.2 Inkommen handling	47
4.4.3 Upprättad handling	48
5 Utlämnande av allmänna handlingar	51
5.1 Bakgrund	51
5.2 Skyndsam handläggning	51
5.3 Anonymitet	52
5.4 Handläggningen av utlämningsärenden i Försvarmakten	52
5.5 Sekretessgranskning	53
5.6 Förbehåll	53
Bilaga 1 - Exempel på avslagsbeslut vid utlämnande av allmän handling	55
Bilaga 2 - Andra staters och mellanfolkliga organisationers motsvarighet till informationssäkerhetsklasser	57
Bilaga 3 - Råd för formulering	59
Fotnoter	61

1 Informationsklassificering i Försvarsmakten

1.1 Försvarsmaktens informationstillgångar

Information är en av Försvarsmaktens viktigaste tillgångar och utgör en förutsättning för att kunna bedriva verksamheten. Myndighetens informationstillgångar måste därför behandlas och skyddas på ett tillfredsställande sätt mot de risker som förekommer i Försvarsmaktens verksamhet. Lagar och förordningar utgör grunden för Försvarsmakten i detta arbete och dessutom ska ingångna internationella överenskommelser och avtal följas.

Med informationstillgångar avses all information oavsett om den behandlas manuellt eller automatiserat och oberoende av i vilken form eller miljö den förekommer. Informationssäkerhet omfattar Försvarsmaktens informationstillgångar utan undantag.³

1.2 Modell för informationsklassificering

Modellen för informationsklassificering i Försvarsmakten utgår från en bedömning av om en uppgift omfattas av sekretess eller inte. Uppgifter vilka omfattas av sekretess indelas i sekretesskategorierna hemliga, utrikesklassificerade respektive sekretessklassificerade uppgifter. Hemliga och utrikesklassificerade uppgifter inplaceras vidare i en av fyra informationssäkerhetsklasser.

I offentlighets- och sekretesslagen (2009:400), OSL, ges bestämmelser om när en uppgift omfattas av sekretess. Denna lag utgör grunden för bedömning av om en uppgift omfattas av sekretess eller inte och är det första steget i klassificering av information.

Om en uppgift omfattas av sekretess och rör *rikets säkerhet* är uppgiften en *hemlig uppgift* enligt säkerhetsskyddsförordningen.⁴ Om en hemlig uppgift är av synnerlig betydelse för rikets säkerhet är uppgiften *kvalificerat hemlig*. För uppgifter som rör rikets säkerhet ska det finnas ett skydd enligt säkerhetsskyddslagstiftningen som benämns *säkerhetsskydd*. Säkerhetsskydd avser främst skydd mot spioneri, sabotage och andra brott som kan hota rikets

säkerhet. Säkerhetsskydd ska även ge ett skydd mot terroristbrott. Hemliga uppgifter ska enligt Försvarsmaktens föreskrifter om säkerhetsskydd placeras i *informationssäkerhetsklass*.⁵ Det finns fyra informationssäkerhetsklasser och dessa är indelade efter vilket *men* som kan uppstå om uppgifterna röjs. Observera att det inte uteslutande är uppgifter som omfattas av försvarssekretess som kan utgöra hemliga uppgifter. Även uppgifter som omfattas av sekretess enligt 15 kap. 1 § OSL (utrikessekretess) och 18 kap. 1 § OSL (förundersökningssekretess) kan i vissa fall vara av betydelse för rikets säkerhet och därmed vara hemliga uppgifter.

Om en uppgift omfattas av sekretess enligt 15 kap. 1 § OSL, s.k. utrikessekretess, men *inte* rör rikets säkerhet, och av annan stat, mellanfolklig organisation eller av svensk myndighet har klassificerats i någon av nivåerna TOP SECRET, SECRET, CONFIDENTIAL eller RESTRICTED eller i motsvarande nivåer på andra språk, så utgör uppgiften en *utrikesklassificerad uppgift* enligt Försvarsmaktens föreskrifter (FFS 2010:1) om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar.⁶ Dessa uppgifter ska också placeras i informationssäkerhetsklass.

Övriga uppgifter vilka omfattas av sekretess, men vilka inte är hemliga eller utrikesklassificerade, benämns *sekretessklassificerade uppgifter* enligt Försvarsmaktens föreskrifter om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar.⁷ Uppgifter i denna sekretesskategori ska *inte* placeras i informationssäkerhetsklass, eftersom uppgifterna varken är hemliga eller utrikesklassificerade. Sekretessklassificerade uppgifter ska däremot ges ett visst skydd vilket framgår av nämnda föreskrifter.

1.3 Ansvaret för informationsklassificering

Den som skapar information genom att upprätta en handling eller på annat sätt sammanställer uppgifter ansvarar även för informationsklassificeringen av uppgifterna. Det är därför viktigt att ha kunskap om de sekretessbestämmelser som är tillämpliga för den information som man hanterar (även sådana som inte är beskrivna i denna handbok) samt om uppgifter i den egna verksamheten kan orsaka men för rikets säkerhet om de röjs och i så fall i vilken omfattning. I verksamhet där det sker ett informationsutbyte med ett annat land eller en mellanfolklig organisation är det också viktigt att känna till det andra landets eller den mellanfolkliga organisationens syn på uppgif-

terna samt motsvarigheter till våra informationssäkerhetsklasser (se bilaga 2), eftersom detta kan påverka vår informationsklassificering.

Vid osäkerhet i informationsklassificeringen ska man vända sig till sin chef eller till organisationsenhetens säkerhetschef för att få stöd med bedömningen.

1.4 Sammanfattning

- Informationsklassificering inleds med att först göra en bedömning om en uppgift omfattas av sekretess eller inte.
- Om uppgiften omfattas av sekretess är nästa steg att bedöma om uppgiften är hemlig eller om den är utrikesklassificerad. I sådana fall fortsätter informationsklassificeringen genom att uppgiften placeras i en informationssäkerhetsklass utifrån det men som ett röjande skulle medföra *eller* utifrån en klassificering som har gjorts av en utländsk myndighet, mellanfolklig organisation eller en svensk myndighet.
- Om det konstateras att en uppgift som omfattas av sekretess inte rör rikets säkerhet och inte är utrikesklassificerad är uppgiften sekretessklassificerad. En sekretessklassificerad uppgift ska inte placeras i informationssäkerhetsklass.

Modellen för informationsklassificering framgår av bild 1.1 nedan. Bilden finns också i inledningen till övriga kapitel av handboken med de för respektive kapitel relevanta delarna av bilden färgmarkerade.

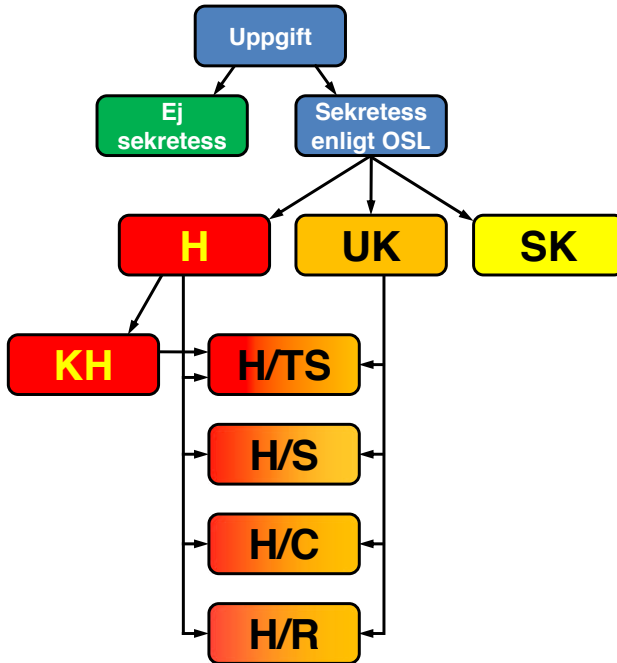


Bild 1.1

2 Offentlighet och sekretess

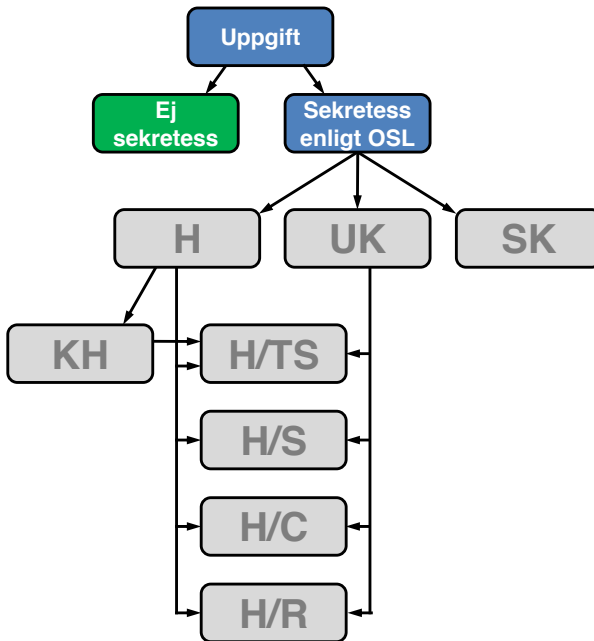


Bild 2.1

2.1 Offentlighetsprincipen

Offentlighetsprincipen, i dess grundläggande form, syftar till att allmänheten ska få insyn i det allmännas verksamhet. Offentlighetsprincipen kommer till uttryck på olika sätt:

- Alla har rätt att ta del av myndigheternas allmänna handlingar (handlingsoffentlighet).
- Anställda i staten och kommunerna har rätt att berätta vad de vet för utomstående (yttrandefrihet för tjänstemän m.fl.).
- Anställda i staten och kommunerna har möjlighet att under vissa förutsättningar lämna uppgifter som omfattas av sekretess till bl.a. tidningar, radio och TV (meddelarfrihet för tjänstemän m.fl.).
- Allmänheten och massmedia har rätt att vara närvarande vid rättegångar samt närvara när riksdagens kammare, kommunfullmäktige, landsting och andra sådana organ sammanträder (förhandlingsoffentlighet).

Den del av offentlighetsprincipen som avser allmänna handlingars offentlighet är grundlagsreglerad i 2 kap. tryckfrihetsförordningen (TF).

2.1.1 Tryckfrihetsförordningen

Med tryckfrihet förstås bl.a. att varje svensk medborgares rätt att, utan några av myndighet eller annat allmänt organ i förväg lagda hinder, ge ut skrifter.⁸ Tryckfrihetsförordningens andra kapitel handlar om rätten att ta del av allmänna handlingar. Rätten gäller såväl för enskilda personer som för den som inom ramen för sitt yrke vill ta del av allmänna handlingar, bl.a. journalister.

Till främjande av ett fritt meningsutbyte och en allsidig upplysning skall varje svensk medborgare ha rätt att taga del av allmänna handlingar.

2 kap. 1 § tryckfrihetsförordningen

Av 14 kap. 5 § TF följer att rätten att ta del av allmänna handlingar inte bara gäller för svenska medborgare utan även för utlänningar.

Rätten att ta del av allmänna handlingar får endast begränsas för i 2 kap. 2 § TF angivna intressen (s.k. sekretessgrunder). Dessa intressen är:

1. rikets säkerhet eller dess förhållande till annan stat eller mellanfolklig organisation,
2. rikets centrala finanspolitik, penningpolitik eller valutapolitik,
3. myndighets verksamhet för inspektion, kontroll eller annan tillsyn,
4. intresset att förebygga eller beivra brott,
5. det allmännas ekonomiska intresse,
6. skyddet för enskilds personliga eller ekonomiska förhållanden och
7. intresset att bevara djur- eller växtart.

Detaljerade bestämmelser om begränsning av rätten att ta del av allmänna handlingar ska enligt TF anges i en särskild lag eller i en annan lag som denna lag hänvisar till. Den lag som avses i TF är offentlighets- och sekretesslagen (2009:400), nedan benämnd OSL. Andra begränsningar i handlingsoffentligheten är i princip otillåtna.

Eftersom rätten att ta del av handlingar är begränsad till allmänna handlingar är det viktigt att känna till dels vad som avses med en handling, dels hur denna handling blir allmän.

2.1.2 En handling

En handling är antingen en framställning i skrift eller bild eller en upptagning som kan läsas, avlyssnas eller på annat sätt uppfattas med ett tekniskt

hjälpmedel. En framställning i skrift eller bild kan exempelvis utgöras av ett handskrivet dokument eller fotografi. En upptagning kan vara en video- eller ljudinspelning, men utgörs oftast av information i ett IT-system, såsom bl.a. textfiler (ordbehandlingsdokument) eller olika former av register.⁹ Begreppet upptagning avser själva informationsinnehållet och inte den fysiska databäraren. I ett IT-system är det således inte alltid hårddisken, disketten, DVD-skivan eller någon annan databärare som utgör en handling. Vanligtvis brukar man beskriva en upptagning som en handling om den utgör en konstellation av uppgifter som har ett sakligt sammanhang. En sådan handling kan exempelvis utgöras av information som finns lagrade på fler än en CD-skiva, medan viss information på samma skiva inte utgör en handling. Det blir därför de lagrade uppgifterna som är handlingar oavsett hur man valt att lagra dessa rent tekniskt. Handlingsbegreppet kan därför i IT-sammanhang få en mycket varierande innebörd.

2.1.3 Allmän handling

En handling är allmän om den förvaras hos en myndighet och antingen är inkommen till myndigheten eller upprättad hos myndigheten¹⁰. För att en handling ska anses vara förvarad hos myndigheten ska den finnas tillgänglig för myndigheten. Är en handling inte tillgänglig för myndigheten så är den följaktligen inte heller en allmän handling hos den myndigheten. En handling som förvaras hos t.ex. en konsult ska däremot anses förvarad vid myndigheten eftersom myndigheten anses ha tillgång till handlingen.

För att en handling ska anses vara inkommen till en myndighet ska den på något sätt ha skickats eller överlämnats till myndigheten. Det är därför viktigt att inkomststämpla och diarieföra alla handlingar som kommer in till myndigheten. Även om en tjänsteman inte har hunnit läsa en inkommen handling, eller om den inte hunnit bli diarieförd, så är handlingen ändå allmän. Sättet den har kommit in på saknar betydelse. När en handling har överlämnats till en behörig tjänsteman vid myndigheten, anses handlingen vara inkommen till myndigheten även om det sker utanför myndighetens lokaler. En sådan handling ska i Försvarsmakten diarieföras så snart som möjligt.

En handling som är upprättad hos en myndighet är också en allmän handling. En handling anses vara upprättad när den har expedierats eller fått sin slutliga utformning. På samma sätt som när det gäller inkomna handlingar, saknar sättet som handlingen har expedierats på betydelse för bedömningen om handlingen är allmän eller inte. Det innebär att även handlingar som överlämnas till mottagare utanför myndigheten anses expedierade och ska därmed också diarieföras som sådana.

När det gäller hantering av exempelvis e-post gäller alltså samma bestämmelser som för pappersdokument. Det betyder att kriterierna förvarad, inkommen och upprättad är tillämpliga även för e-post. Innebörden av detta är att e-post kan komma att lämnas ut till en sökande om inte sekretess hindrar det.

Från allmänna handlingar undantas bl.a. handlingar som är ställda till personer som innehavare av annan ställning än som tjänsteman, t.ex. som privatperson eller som facklig förtroendeman. Observera att en handling som innehåller både information gällande tjänsten och information av privat karaktär i sin helhet blir en allmän handling.¹¹ Detta kan få betydelse i t.ex. e-postsammanhang där privata meddelanden blandas med information för myndighetens verksamhet.

Exempel 2.1

Som exempel kan anges att du skickar ett e-postmeddelande till en kollega och frågar om ni ska äta lunch tillsammans. Detta meddelande är privat och behöver därför inte lämnas ut. Om du däremot i samma meddelande avslutar med att ta upp någon fråga som rör tjänsten, blir hela meddelandet allmän handling och kan vid en begäran lämnas ut i sin helhet.

Ett e-postmeddelande är att betrakta som inkommet till myndigheten i det ögonblick då det finns tillgängligt på en e-postserver som myndigheten förfogar över. Det krävs alltså inte att en berörd befattningshavare har öppnat meddelandet och tagit del av innehållet för att meddelandet ska anses vara inkommet. När den anställde använder Internet blir även s.k. cookie-filer, som bl.a. visar vilka webbplatser denne har besökt, allmänna handlingar. Det kan dock tilläggas att cookie-filer, global- och historikfiler normalt inte behöver sparas eftersom de oftast saknar betydelse för myndighetens verksamhet och därför får gallras.

2.1.4 Arbetshandlingar

Minnesanteckningar, utkast, privata brev, underhandsremisser och koncept till en myndighets beslut är inte allmänna handlingar, om dessa inte expedierats eller tagits om hand för arkivering.¹² Med minnesanteckningar avses synpunkts- och föredragningspromemorior, sammanställningar av svåröverskådligt material och andra anteckningar som görs under beredningen av ett ärende. Utmärkande för denna typ av handlingar är att de har tillkommit som hjälpmedel vid beredning och föredragning av ett ärende. Utkast och koncept (s.k. mellanprodukter) kännetecknas av att de utgör förstadiet till en slutligt utformad handling. Med underhandsremiss menas utkast, koncept eller andra handlingar som är under bearbetning och som skickas till en annan myndighet *endast* i samrådssyfte. Denna typ av handlingar är inte allmänna och behöver därför inte lämnas ut till allmänheten.

2.2 Sekretess

2.2.1 Beskrivning av sekretess

Sekretess innebär ett förbud att röja en uppgift muntligen (tystnadsplikt) eller genom att allmän handling lämnas ut (handlingssekretess) eller att det sker på annat sätt.¹³ Exempel på andra sätt att röja en uppgift kan vara uppvisande av hemlig materiel för obehöriga, utlämnande av en hemlig handling¹⁴ som inte är allmän eller att en uppgift som omfattas av sekretess sänds i ett e-postmeddelande. När sekretess för en uppgift gäller enligt en bestämmelse i OSL begränsas allmänhetens rätt att ta del av en allmän handling där uppgiften förekommer. Sekretess innebär även att de som är behöriga att hantera uppgifterna inte muntligen eller på annat sätt får röja uppgifterna. Ansvarsbestämmelser om detta finns i reglerna om brott mot tystnadsplikten i 20 kap. 3 § brottsbalken. Att felaktigt lämna ut en handling som på grund av sekretess inte får lämnas ut kan även utgöra tjänstefel enligt 20 kap. 1 § brottsbalken.

Sekretess gäller för en *uppgift* oavsett i vilken form uppgiften förekommer. Sekretessen avser således inte enbart uppgifter i allmänna handlingar utan all förekomst av dessa uppgifter.

Sekretessen gäller gentemot enskilda, mot andra myndigheter och även gentemot olika verksamhetsgrenar inom en myndighet om de är att betrakta som självständiga i förhållande till varandra. Det finns undantag mot detta och i vissa fall får myndigheter lämna uppgifter som omfattas av sekretess till andra myndigheter t.ex. när det är nödvändigt att den utlämnande myndigheten ska kunna fullgöra sin verksamhet (se exempel 2.2), eller om utlämnandet sker med stöd av lag eller förordning. I OSL¹⁵ finns ytterligare föreskrifter om under vilka förutsättningar vissa uppgifter som omfattas av sekretess får lämnas till bl.a. andra myndigheter.

Exempel 2.2

I Försvarsmakten finns en handling som innehåller en kravspecifikation på ett framtida vapensystem. Dessa uppgifter omfattas av sekretess. Försvarsmakten behöver stöd från Försvarets materielverk avseende upphandlingen av vapensystemet. Normalt hade sekretessen förhindrat Försvarsmakten att lämna uppgifterna till Försvarets materielverk, men i detta fall är utlämnandet nödvändigt för att Försvarsmakten ska kunna fullgöra sin verksamhet och det är därför tillåtet.

Naturligtvis gäller sekretessen även gentemot utländska myndigheter. En svensk myndighet får dock lämna ut uppgifter som omfattas av sekretess till en utländsk myndighet eller en mellanfolklig organisation om:

1. utlämnandet sker i enlighet med särskild föreskrift i lag eller förordning, eller
2. uppgiften i motsvarande fall skulle få lämnas ut till en svensk myndighet och det enligt den utlämnande myndighetens prövning står klart att det är förenligt med svenska intressen att uppgiften lämnas ut.¹⁶

Observera att myndighetens prövning ska ske av överbefälhavaren eller den person han eller hon har delegerat beslutsrätten till.

Ett röjande av uppgifter som omfattas av sekretess till en utländsk myndighet som inte sker i enlighet med ovanstående kan vara brottsligt.

2.2.2 Bedömning av sekretess

För att bedöma om en uppgift omfattas av sekretess används följande metod:

1. Inhämta (vid behov) teoretiska kunskaper om offentlighet och sekretess (kapitel 2 i denna handbok).
2. Kontrollera om uppgiften som ska bedömas omfattas av sekretess, d.v.s. om det finns någon bestämmelse i OSL som är tillämplig för den aktuella uppgiften (kapitel 3 i denna handbok).
3. Bedöm den aktuella uppgiften utifrån den eller de tillämpliga sekretessbestämmelserna och avgör om kriterierna är uppfyllda (vanligen avseende men eller skada).

Vid sekretessprövningen kan myndigheten behöva rådgöra med andra myndigheter för att kunna bedöma om skaderekvisiten är uppfyllda. Observera att sekretessen i varje enskilt fall ska kunna motiveras utifrån en uttrycklig sekretessbestämmelse i OSL.

Sekretessbestämmelserna i OSL är uppbyggda kring olika villkor som ska vara uppfyllda för att sekretess ska gälla för en uppgift. Ett villkor kan vara att uppgiften ska förekomma inom en viss verksamhet, t.ex. inom hälso- och sjukvård. Ett annat villkor kan vara att uppgiften ska finnas vid vissa utpekade myndigheter. Andra sekretessbestämmelser är mer generellt utformade och begränsas inte till verksamheter eller särskilt angivna myndigheter. Ett exempel på detta är försvarssekretessen.¹⁷ De flesta sekretessbestämmelser

anger de villkor som krävs för att bestämmelsen ska vara tillämplig (s.k. skaderekvisit).

I OSL finns två huvudtyper av skaderekvisit – *rakt* respektive *omvänt* skaderekvisit.

Rakt skaderekvisit	Rakt skaderekvisit innebär att <i>offentlighet</i> gäller som huvudregel för en uppgift och att sekretess enbart gäller under förutsättning att ett röjande kan leda till det men eller den skada som beskrivs i bestämmelsen.
Omvänt skaderekvisit	Omvänt skaderekvisit innebär att <i>sekretess</i> gäller som huvudregel för en uppgift och att offentlighet enbart gäller under förutsättning att ett röjande <i>inte</i> kan leda till det men eller den skada som beskrivs i bestämmelsen.

När det saknas ett angivet skaderekvisit i en sekretessbestämmelse är sekretessen ovillkorlig för uppgiften i sekretessbestämmelsen. Sekretess gäller i sådant fall för den beskrivna typen av uppgifter oavsett om ett röjande medför en skada eller inte. Sådana sekretessbestämmelser anses beskriva att *absolut sekretess* föreligger för uppgifterna. Denna typ av bestämmelse är dock ovanlig.

2.2.3 Sekretessmarkering

En handling som innehåller en uppgift som kan antas omfattas av sekretess får förses med en särskild anteckning – sekretessmarkering.¹⁸ Denna markering ska innehålla följande uppgifter:

1. Tillämplig sekretessbestämmelse,
2. datum när anteckningen gjordes, och
3. den myndighet som har gjort anteckningen.

Enligt OSL är det inte obligatoriskt för myndigheterna att göra någon sekretessmarkering, men vissa myndigheter kan ha interna bestämmelser som föreskriver att sekretessmarkering alltid ska ske för vissa typer av uppgifter. I Försvarsmakten ska allmänna handlingar som innehåller uppgifter som omfattas av sekretess förses med sekretessmarkering. Även handlingar som inte är allmänna ska märkas på lämpligt sätt.¹⁹



Bild 2.2. Exempel på sekretessmarkeringar i Försvarsmakten.

Det förekommer att handlingar inkommer till Försvarsmakten som, trots att de innehåller uppgifter som omfattas av sekretess, inte är försedda med sekretessmarkering. Försvarsmakten ska därför självständigt bedöma sekretessen för varje inkommen handling och vid behov förse handlingen med tillämplig markering.

2.2.4 Rätten att meddela och offentliggöra uppgifter

Rätten att meddela och offentliggöra uppgifter, även kallad meddelarfrihet, är en rättighet som regleras i två av våra grundlagar.²⁰ Meddelarfrihet innebär att alla medborgare får lämna vissa uppgifter som omfattas av sekretess till t.ex. journalister och författare för publicering i tryckt skrift, radio eller TV. Det ställs två krav som måste vara uppfyllda för att meddelarfriheten ska gälla. För det första måste uppgiften lämnas till en journalist, författare eller motsvarande och för det andra krävs att uppgiften lämnas i syfte att offentliggöras. Att avslöja en uppgift som omfattas av sekretess för en kollega eller för någon i sin bekantskapskrets är inte tillåtet eftersom det i dessa fall inte är fråga om den behöriga kretsen av mottagare till informationen och att ett syfte att offentliggöra uppgiften inte föreligger. Uppgifter får lämnas muntligen eller skriftligen, men allmänna handlingar får inte lämnas ut. Att således lämna ut uppgifter som omfattas av sekretess genom att lämna ut en allmän handling som innehåller dessa uppgifter omfattas *inte* av tryckfrihetsförordningens bestämmelser om meddelarfrihet.

Det bör noteras att det är fråga om en *rättighet* att använda sig av meddelarfriheten och det finns naturligtvis ingen *skyldighet* att lämna ut uppgifter som omfattas av sekretess till massmedia på den grunden. Det är den enskilde tjänstemannen som avgör om han eller hon vill nyttja sin meddelarfrihet. Den omständigheten att det finns en särskild pressansvarig vid myndigheten innebär inte att de anställda får hindras att nyttja sin yttrandefrihet eller meddelarfrihet.

Det är självklart att meddelarfrihet inte kan gälla fullt ut. Det finns områden där intresset av sekretessen väger tyngre än kravet på offentlig insyn. De undantag från meddelarfriheten som finns anges i 7 kap. 3 § TF samt de kapitel i OSL som innehåller sekretessbestämmelser. Under beskrivningen av sekretessbestämmelserna i kapitel 3 beskrivs meddelarfriheten utifrån vad som gäller specifikt för varje särskild sekretessbestämmelse.

3 Beskrivning av sekretessbestämmelser

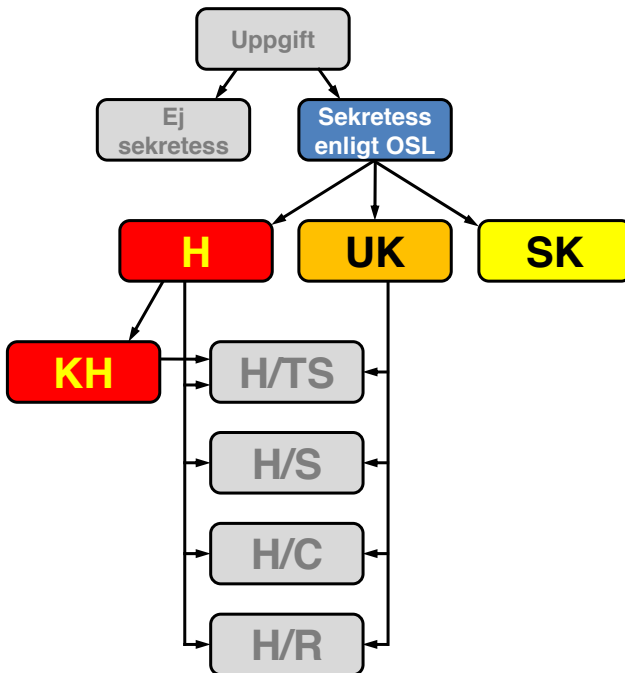


Bild 3.1

3.1 Inledning

Den 30 juni 2009 trädde offentlighets- och sekretesslagen (2009:400) OSL, i kraft. Den nya lagen är en omarbetning av den gamla sekretesslagen från 1980 och syftar till att göra regleringen mer lättförståelig och lättillämpad. OSL har fått en ny struktur och innehållsförteckning, kortare paragrafer och ett något upplättat språk. För anställda i Försvarsmakten innebär den nya lagen en ominläring av de sekretessbestämmelser som är aktuella i verksamheten. Ominläringen innefattar enbart de nya paragrafnumreringarna. I detta kapitel ges en beskrivning av fem utvalda sekretessbestämmelser som har bedömts vara de som oftast förekommer i Försvarsmaktens verksamhet. Det bör påpekas att det för vissa verksamheter i Försvarsmakten finns andra sekretessbestämmelser som är tillämpliga. Tabellen nedan syftar till att ge en överblick av kapitlens upplägg men även förenkla inläringen av de nya paragrafnumreringarna. För övriga sekretessbestämmelser hänvisas till OSL.

Bestämmelsen i 18 kap. 8 § OSL rubriceras i lagen som "Säkerhets- eller bevakningsåtgärd". I denna handbok kallas bestämmelsen "Säkerhets- och bevakningssekretess". Bestämmelsen i 19 kap. 3 § OSL har i lagen rubriken "Upphandling m.m.", men kallas "Upphandlingssekretess" i denna handbok. Avslutningsvis benämns bestämmelsen i 31 kap. 16 § OSL "Affärsförbindelse med myndighet", men kallas i denna handbok "Affärssekretess". Dessa benämningar har valts att användas i handboken i syfte att förenkla de olika sekretessuttrycken för användarna.

Sekretessbestämmelse i OSL	Område
15 kap. 2 §	Försvarssekretess
15 kap. 1 §	Utrikessekretess
18 kap. 8 §	Säkerhets- och bevakningssekretess
19 kap. 3 §	Upphandlingssekretess
31 kap. 16 §	Affärssekretess

3.2 Försvarssekretess

Sekretess gäller för uppgift som rör verksamhet för att försvara landet eller planläggning eller annan förberedelse av sådan verksamhet eller som i övrigt rör totalförsvaret, om det kan antas att det skadar landets försvar eller på annat sätt vållar fara för rikets säkerhet om uppgiften röjs.

För uppgift i en allmän handling gäller sekretessen i högst fyrtio år.

15 kap. 2 § offentlighets- och sekretesslagen
(utdrag ur första och andra styckena)

3.2.1 Tillämpning av försvarssekretess

Bestämmelsen om försvarssekretess har sitt största tillämpningsområde i fråga om uppgifter som avser det militära försvaret. Med *landets försvar* avses alla de olika verksamheter som är av betydelse för landets samlade försvarsåtgärder, alltså inte bara rent militära företeelser utan också åtgärder med avseende på totalförsvaret i övrigt. Samtliga uppgifter rörande Försvarsmaktens verksamhet, allt från de första förberedelserna till verkställighet och uppföljning, omfattas av bestämmelsen om försvarssekretess. Uppgifter om förhållanden i naturen som är av betydelse ur försvarssynpunkt kan också

vara föremål för sekretess enligt denna bestämmelse. Det kan exempelvis gälla lägesbestämd information om förhållanden på och under markytan samt på och under sjö- och havsbotten som kan antas medföra skada för Sveriges totalförsvaret om uppgifterna röjs.²¹

För att undvika ett onödigt hemlighållande av uppgifter på de många verksamhetsområden som försvarssekretessen omfattar, har bestämmelsen utformats med ett rakt skaderekvisit, dvs. att offentlighet gäller som huvudregel. Det har ansetts att samhällets åtgärder för landets försvar inte ska undandras offentlighet annat än när det verkligen är påkallat. Försvarssekretessen gäller därför bara om det kan antas att ett röjande av uppgifterna skadar landets försvar eller på annat sätt vållar fara för rikets säkerhet.

De villkor som gäller för att försvarssekretessen ska vara tillämplig är dels att en uppgift ska röra *verksamhet, planläggning* eller annan *förberedelse* för att *försvaret* eller i övrigt röra *totalförsvaret*, dels att uppgiften kan *antas skada landets försvar* eller *på annat sätt vålla fara för rikets säkerhet*.

För att en uppgift ska rymmas i sekretessområdet krävs att ett röjande av uppgiften innebär en minskad förmåga att försvaret (avser främst det militära försvaret) eller minskade möjligheter att uthärda ett krig (till exempel försörjningsfrågor). Uppgifter inom det civila försvaret kan också omfattas av försvarssekretess om uppgifterna rör verksamhet som behövs för att förbereda det civila samhället för krig. Om det kan antas att ett röjande av en uppgift leder till att Sverige får minskad försvarsförmåga, försvarsvilja eller eliminerar eller minskar effekten av ett framtaget försvarssystem, så anses ett sådant röjande skada landets försvar. En sådan uppgift omfattas således av försvarssekretess.

3.2.2 Totalförsvaret

Totalförsvaret definieras i 1 § lag (1992:1403) om totalförsvaret och höjd beredskap som *verksamhet som behövs för att förbereda Sverige för krig*. Totalförsvaret består av militär verksamhet (militärt försvar) och civil verksamhet (civilt försvar).

Totalförsvarets resurser ska förutom i krig även kunna användas vid internationella fredsfrämjande och humanitära insatser och för att stärka samhällets förmåga till att förebygga och hantera svåra påfrestningar på samhället i fred. När totalförsvarets resurser används i sådan verksamhet utgör verksamheten dock inte totalförsvarets verksamhet.²² Att Försvarsmakten använder personal och materiel, som är avsedda för försvaret av Sverige, i en internationell fredsfrämjande insats utomlands innebär inte att insatsen är totalförsvarets verksamhet.

Uppgifter om en internationell fredsfrämjande insats omfattas normalt inte av sekretess enligt 15 kap. 2 § OSL eftersom insatsen inte rör verksamhet för att försvara landet eller i övrigt rör totalförsvaret. Däremot kan uppgifter om de totalförsvaresresurser som används i en sådan insats omfattas av försvarssekretess. Ett exempel på detta är egenskaper i kvalificerade vapen- eller sensorsystem.

3.2.3 Försvarssekretess och rikets säkerhet

Begreppet *rikets säkerhet* är inte definierad i lagstiftningen. Innebörden får därför bestämmas utifrån förarbeten, rättspraxis och myndigheternas tillämpning. Med rikets säkerhet brukar avses såväl den *yttre säkerheten* för det nationella oberoendet (främst totalförsvaret) som den *inre säkerheten* för det demokratiska statsskicket.²³ Av straffbestämmelserna i 19 kap. brottsbalken om brott mot rikets säkerhet följer att de skyddsvärda intressen som omfattas av begreppet rikets säkerhet utgörs av Sveriges integritet, rikets oberoende och fortbestånd samt dess demokratiska statsskick.

Begreppet rikets säkerhet är dessutom av central betydelse för att avgöra om en uppgift som omfattas av sekretess ska omfattas av ett säkerhetsskydd eller inte. I 4 § säkerhetsskyddsförordningen (1996:633) definieras *hemlig uppgift* som uppgift som omfattas av sekretess enligt OSL och som rör rikets säkerhet. Uppgifter som omfattas av försvarssekretess rör alltid rikets säkerhet och är därmed hemliga uppgifter. Sådana uppgifter ska alltid placeras i informationssäkerhetsklass.

3.2.4 Sekretesstider

Sekretesstiden för uppgifter i allmänna handlingar som omfattas av försvarssekretess är som huvudregel högst 40 år. När det i en allmän handling förekommer vissa i offentlighets- och sekretessförordningen särskilt angivna uppgifter som omfattas av försvarssekretess kan längre sekretesstider gälla. T.ex. om en sådan uppgift rör landskapsinformation om militärgeografiska förhållanden, rikets fasta försvarsanläggningar för krigsbruk eller underhållsanläggningar som kan röja försvarets grupperingar, är sekretesstiden högst 150 år. Samma sekretesstid gäller för planerade försvarsanläggningar i form av mineringar och andra hinder. Om det i en allmän handling förekommer uppgifter som rör underrättelseverksamheten inom underrättelse- och säkerhetstjänsten eller militärtekniska forskningsresultat är sekretesstiden högst 70 år.²⁴

3.2.5 Rätten att meddela och offentliggöra uppgifter

Rätten att meddela uppgifter för offentliggörande och offentliggöra uppgifter i tryckt skrift eller i vissa andra medier, den s.k. meddelarfriheten, regleras i tryckfrihetsförordningen (TF)²⁵ och i yttrandefrihetsgrundlagen (YGL).²⁶

I tryckfrihetsförordningen regleras även de fall där meddelarfriheten inte gäller.²⁷ För uppgifter som omfattas av försvarssekretess är meddelarfriheten starkt inskränkt. Meddelarfrihet föreligger exempelvis inte när någon har betrotts en uppgift i tjänsten.²⁸ Se även avsnitt 2.2.4.

3.2.6 Sammanfattning

- Försvarssekretess gäller för uppgift som rör verksamhet eller planläggning eller förberedelse för att försvara landet.
- Försvarssekretess gäller också för uppgift som i övrigt rör totalförsvaret.
- Försvarssekretess gäller dock enbart om det kan antas att det skadar landets försvar eller på annat sätt vållar fara för rikets säkerhet om uppgiften röjs.
- Försvarssekretess kan vara tillämplig i såväl Försvarmaktens nationella som dess internationella verksamhet.

3.3 Utrikessekretess

Sekretess gäller för uppgift som rör Sveriges förbindelser med en annan stat eller i övrigt rör annan stat, mellanfolklig organisation, myndighet, medborgare eller juridisk person i annan stat eller statslös, om det kan antas att det stör Sveriges mellanfolkliga förbindelser eller på annat sätt skadar landet om uppgiften röjs.

För uppgift i en allmän handling gäller sekretessen i högst fyrtio år.

15 kap. 1 § offentlighets- och sekretesslagen

3.3.1 Tillämpning av utrikessekretess

Föremålet för utrikessekretessen är först och främst uppgifter som rör Sveriges förbindelser med annan stat. Härmed avses inte bara uppgifter om de egentliga utrikespolitiska förbindelserna utan också handelsförbindelser, kulturella förbindelser m.m. I uttrycket *Sveriges förbindelser* ligger att det måste röra sig om förbindelser på nationell nivå. En svensk myndighets kontakter med en främmande stat ryms inte under uttrycket, om förbindelserna avser myndighetens egna angelägenheter. Företräder däremot myndigheten Sverige som nation t.ex. vid en förhandling av ett internationellt avtal, rör det sig om Sveriges förbindelser med en annan stat.

Försvarsmaktens samarbete med andra stater eller mellanfolkliga organisationer kan komma att omfattas av denna bestämmelse. Detta på grund av att Försvarsmakten i sådana fall handlar på uppdrag av regeringen, och således representerar Sverige som nation.

Bestämmelsen om utrikessekretess har sin största betydelse för regeringen, Regeringskansliet och utrikesrepresentationen, men den omfattar också samtliga statliga myndigheter. Med utrikesrepresentationen avses svenska beskickningar, konsulat och delegationer hos mellanfolkliga organisationer såsom FN, NATO, Europarådet och EU. Tillämpning av utrikessekretessen kan ibland präglas av hänsynstaganden på politisk nivå. För att få full förståelse för att kunna bedöma om sekretess gäller i det enskilda fallet krävs som regel en kännedom om de politiska förhållanden som rör Sveriges relationer med den främmande staten eller mellanfolkliga organisationen.

Bestämmelsen om utrikessekretess är utformad med ett rakt skaderekvisit. Detta innebär att huvudregeln är offentlighet. Det ska dock göras en prövning om ett röjande av uppgiften kan antas störa Sveriges mellanfolkliga

förbindelser eller på annat sätt skadar landet. Den i Sverige grundlagsfästa offentlighetsprincipen och offentlighets- och sekretesslagstiftningen är i många delar unik och kan upplevas som mycket långtgående av andra stater och mellanfolkliga organisationer som ofta har en annan syn på sekretess och offentlighet än vad Sverige har. Det är därför viktigt att beakta detta vid en bedömning om ett offentliggörande av en uppgift kan störa Sveriges mellanfolkliga förbindelser.

Enligt regeringsformen²⁹ ska statliga myndigheter informera utrikesministern när det uppstår en fråga som är av betydelse för Sveriges förhållande till annan stat eller mellanfolklig organisation. Denna bestämmelse kan aktualiseras t.ex. när Försvarsmakten ska avgöra om en uppgift som rör Sveriges förbindelser med annan stat omfattas av utrikessekretess.

3.3.2 Hantering av utländska uppgifter

Handlingar som Försvarsmakten *får* från andra stater eller mellanfolkliga organisationer och som försetts med beteckningar som anger att handlingen innehåller uppgifter som omfattas av sekretess enligt den andra statens eller mellanfolkliga organisationens regler, omfattas normalt av utrikessekretess. Det kan sannolikt antas att ett röjande av dessa utländska uppgifter skulle störa Sveriges förbindelser med den staten eller mellanfolkliga organisationen. Ett röjande av sådana uppgifter kan innebära att det aktuella landet avbryter ett pågående projekt eller samarbete, får minskat förtroende för Sverige eller inte längre lämnar uppgifter som omfattas av sekretess till Sverige.

Sverige har ingått ett antal olika internationella säkerhetsskyddsavtal med andra stater där nationerna gemensamt har förbundit sig till att skydda varandras uppgifter som omfattas av sekretess enligt det upprättande landets beteckning. Detta innebär bl. a. att om Sverige får en handling som är märkt SECRET (eller motsvarande) från en annan stat, kan utrikessekretess gälla för denna handling. Ett sådant avtal innebär inte att handlingen eller uppgiften i fråga är undantagen offentlighetsprincipen. Således ska en sedvanlig sekretessprövning göras beträffande samliga uppgifter i en sådan handling.

Handlingar från andra stater eller mellanfolkliga organisationer kan vara försedda med beteckningar som anger att handlingen innehåller uppgifter som omfattas av sekretess enligt den andra statens eller mellanfolkliga organisationens regler, men som *inte* ska ges ett särskilt skydd. Exempel på sådana beteckningar är NATO UNCLASSIFIED, LIMITE, som förekommer i EU, och Controlled Unclassified Information, som förekommer i USA. Uppgifter i sådana handlingar omfattas normalt av utrikessekretess och ska i Försvarsmakten klassificeras som *sekretessklassificerade* handlingar.

Utrikessekretess kan även gälla för uppgifter i de handlingar som Försvarsmakten *upprättar* om annan stat, mellanfolklig organisation, myndighet, medborgare eller juridisk person i annan stat eller statslös, om det kan antas att ett röjande stör Sveriges mellanfolkliga förbindelser eller på annat sätt skadar Sverige. Vid Försvarsmaktens olika samarbeten med andra stater eller mellanfolkliga organisationer, t.ex. inom försvarsindustrin, övningsverksamhet, utbildning eller fredfrämjande insatser, kan uppgifter i handlingar som *upprättas inom detta samarbete* omfattas av utrikessekretess. En vägledning ifråga om tillämpning av utrikessekretess kan vara vad de olika samarbetsparterna har för uppfattning om eventuella konsekvenser för det fall uppgifter som hanteras inom det samarbetet skulle röjas.

Uppgifter som omfattas av utrikessekretess kan vara av betydelse för rikets säkerhet och utgör då *hemliga* uppgifter. Dessa uppgifter ska placeras i informationssäkerhetsklass. Om uppgifterna inte rör rikets säkerhet men av ett annat land eller mellanfolklig organisation som Sverige har en säkerhetsskyddsavtal med har åsatts en markering på nivåerna TOP SECRET, SECRET, CONFIDENTIAL eller RESTRICTED (eller motsvarande) är dessa *utrikesklassificerade*³⁰ uppgifter. Dessa uppgifter ska placeras i informationssäkerhetsklass.

En svensk myndighet kan också inom ramen för ett internationellt samarbete upprätta handlingar som omfattas av utrikessekretess och som ska delges till andra länder eller mellanfolkliga organisationer. Om det inom detta samarbete finns bestämmelser om hur informationen ska klassificeras och märkas ska handlingen klassificeras och förses med en sådan märkning. Sådana handlingar är i Försvarsmakten *utrikesklassificerade* handlingar och ska placeras i den informationssäkerhetsklass som motsvarar den internationella eller utländska klassificeringen.

3.3.3 Utrikessekretess och rikets säkerhet

Uppgifter som omfattas av utrikessekretess bedöms mycket sällan röra rikets säkerhet. Sådana uppgifter kan dock förekomma t.ex. vid förberedelser för försvaret av Sverige som inbegriper stöd från andra stater eller mellanfolkliga organisationer. Ett annat exempel på när utrikessekretessen skulle kunna röra rikets säkerhet är sådana uppgifter som om de röjs medför att Sverige vid ett eventuellt krig får sämre möjlighet att försvara sig eller svårare att hålla sig utanför ett krig. Ytterligare ett exempel på situationer när utrikessekretessen kan röra rikets säkerhet är om Sverige bedriver gränsförhandlingar med en annan stat där ett röjande av svenska förhandlingsdirektiv kan antas innebära

fara för rikets oberoende eller bestånd.³¹ Övervägande delen av de uppgifter som omfattas av utrikessekretess, till exempel inom ramen för Försvarsmaktens deltagande i multinationella insatser, rör dock inte rikets säkerhet.

Sverige har genom säkerhetsskyddsavtal med vissa stater och mellanfolkliga organisationer kommit överens om att skydda utländska uppgifter på samma sätt som man skyddar uppgifter som rör rikets säkerhet. När Försvarsmakten får en handling från en annan stat eller mellanfolklig organisation och den staten eller organisationen har placerat handlingen i deras motsvarighet till informationssäkerhetsklass, innebär det inte att handlingen rör rikets säkerhet. Det är inte den andra statens eller mellanfolkliga organisationens märkning av handlingen som avgör om den rör rikets säkerhet, utan enbart om uppgifterna i handlingen har betydelse för antingen den yttre eller inre säkerheten i Sverige.

3.3.4 Rätten att meddela och offentliggöra uppgifter

Rätten att meddela och offentliggöra uppgifter i tryckt skrift eller i vissa andra medier, den s.k. meddelarfriheten, regleras i tryckfrihetsförordningen³² (TF) och i yttrandefrihetsgrundlagen³³ (YGL). För uppgifter som omfattas av utrikessekretess råder tystnadsplikt som inskränker denna rättighet.³⁴ En förutsättning för att denna tystnadsplikt ska inskränka meddelarfriheten är att det är fråga om en uppgift vars röjande kan *antas sätta rikets säkerhet i fara* eller annars *skada landet allvarligt*. Meddelarfrihet råder således för uppgifter som omfattas av utrikessekretess, under förutsättning att man kan konstatera att ett röjande inte kan antas sätta Sveriges säkerhet i fara eller annars skada landet allvarligt.

Som ett exempel kan nämnas att det vid ett offentliggörande av en uppgift föreligger en risk för att Sverige hamnar i underläge i en för landet betydelsefull handelsförhandling eller en påtaglig försämring av relationerna med en annan stat, med vilken Sverige i övrigt har betydelsefulla förbindelser. I ett sådant fall gäller inte meddelarfrihet för uppgifter som omfattas av utrikessekretess.

Det ska dock påpekas att, när den enskilde överväger att meddela och offentliggöra uppgifter som omfattas av utrikessekretess, måste han eller hon göra en bedömning om ett sådant röjande kan antas sätta Sveriges säkerhet i fara eller annars skada landet allvarligt. Det kan ytterst komma att vara en domstol som avgör om den som har lämnat en uppgift till exempelvis en journalist har förfarit straffbart eller inte. Se även avsnitt 2.2.4

3.3.5 Sammanfattning

- Utrikessekretess gäller när man kan anta att ett röjande av en uppgift stör Sveriges internationella förbindelser.
- Utrikessekretess gäller också vid de situationer där man kan anta att ett röjande av en uppgift på annat sätt kan skada Sverige.
- Utrikessekretess är aktuell främst vid Försvarsmaktens internationella verksamhet och samarbeten.
- Utrikessekretess rör sällan rikets säkerhet.

3.4 Säkerhets- och bevakningssekretess

Sekretess gäller för uppgift som lämnar eller kan bidra till upplysning om säkerhets- eller bevakningsåtgärd, om det kan antas att syftet med åtgärden motverkas om uppgiften röjs och åtgärden avser

1. byggnader eller andra anläggningar, lokaler eller inventarier,
2. tillverkning, förvaring, utlämning eller transport av pengar eller andra värdeföremål samt transport eller förvaring av vapen, ammunition, sprängämnen, klyvbart material eller radioaktiva ämnen,
3. telekommunikation eller system för automatiserad behandling av information,
4. behörighet att få tillgång till upptagning för automatiserad behandling eller annan handling,
5. den civila luftfarten eller den civila sjöfarten,
6. transporter på land av farligt gods, eller
7. hamnskydd.

18 kap. 8 § offentlighets- och sekretesslagen

3.4.1 Tillämpning av säkerhets- och bevakningssekretess

I denna paragraf finns bestämmelser om sekretess för olika brottsförebyggande åtgärder som i huvudsak hänför sig till annan verksamhet än polisens. Vissa av åtgärderna syftar endast indirekt till att förebygga brott. Sekretessen enligt alla punkter i bestämmelsen är begränsad genom ett rakt skaderekvisit.

Således gäller även här att offentlighet är huvudregel. För sekretess krävs att det vid en prövning ska kunna antas, att ett röjande av uppgiften motverkar syftet med säkerhets- eller bevakningsåtgärden. Uppgifter om säkerhets- eller bevakningsåtgärder kan även omfattas av försvars- eller utrikessekretess. En förutsättning för detta är dock att uppgifterna uppfyller villkoren i respektive sekretessbestämmelse.

I Försvarsmakten torde teknisk anläggningsdokumentation³⁵ i stor utsträckning innehålla uppgifter som omfattas av bestämmelsen om säkerhets- och bevakningssekretess. Sekretessen är inte begränsad till att omfatta säkerhets- eller bevakningsåtgärder i Försvarsmakten utan omfattar även uppgifter som förekommer hos Försvarsmakten om andra myndigheters eller enskildas säkerhets- eller bevakningsåtgärder. Uppgifter som omfattas av bevaknings- och säkerhetssekretess kan enbart utgöra *sekretessklassificerade*³⁶ uppgifter. Om uppgifterna rör t.ex. försvarsanläggningar kan dock försvarssekretess gälla parallellt för uppgifterna.

3.4.2 Byggnader, anläggningar, lokaler och inventarier

I paragrafens första punkt behandlas byggnader eller andra anläggningar, lokaler eller inventarier. Med anläggningar avses bl.a. kulvertsystem, upp- lag och uppställningsplatser. Det är således inte enbart utrymmen med en omslutningsyta (huskropp, berganläggning eller motsvarande) som omfattas utan även öppna inhägnade ytor. Säkerhets- eller bevakningsåtgärder för byggnader, anläggningar och lokaler avser utformningen av tillträdesbegränsning som ska hindra att obehöriga får tillträde till utrymmen eller att upptäcka obehöriga.³⁷ Dessa åtgärder kan även omfatta sådana åtgärder som syftar till att hindra eller upptäcka avlyssning.

Exempel på säkerhets- eller bevakningsåtgärder är byggnadstekniska åtgärder (mekaniskt inbrottskydd), teknisk bevakning (inbrottslarm, passerkontroll och övervakningssystem) och manuell bevakning. Byggnadsritningar och projekteringshandlingar för exempelvis inbrottslarm som kartlägger säkerhetsåtgärder eller säkerhetsbrister är också sådana uppgifter som kan omfattas av den aktuella bestämmelsen. Ytterligare ett exempel på uppgifter för vilka sekretess kan gälla enligt denna punkt är sådana uppgifter om konstruktionen av Försvarsmaktens högkvartersbyggnad. Om sådana uppgifter som rör säkerheten röjs, kan det antas att syftet med skyddsåtgärderna motverkas. Sekretessen kan även gälla uppgifter om instruktioner och tjänstgöringslistor som rör bevakningen av en byggnad.

3.4.3 Telekommunikation och IT-system

Säkerhets- och bevakningssekretessens tredje punkt behandlar *telekommunikation* med vilket avses överföring av meddelanden med telefoni, tråd, radio eller liknande metod. Syftet med att skydda telekommunikationer är att hindra brott mot rikets säkerhet samt sabotage³⁸ eller brytande av post- eller telehemlighet.³⁹ Sekretessbestämmelsen syftar även till att skydda data- och telekommunikationer för att t.ex. hindra brott mot rikets säkerhet.

Sekretessen avser uppgifter som rör skyddet för telekommunikation som, om de röjs, kan leda till att syftet med säkerhetsåtgärderna motverkas. Uppgifterna kan avse såväl fysiska som logiska företeelser. Exempel på uppgifter som kan omfattas av sekretessen är frekvenser och sändningsmetoder för radiokommunikation, adressinformation i tele- och datakommunikationsnätverk t.ex. telefonnummer och IP-adresser. Ytterligare exempel på uppgifter som kan omfattas av sekretessen är framföringsvägar för kablar för telekommunikation till en anläggning som Försvarsmakten disponerar.

Sekretessbestämmelsen ska inte tillämpas på alla uppgifter enligt ovan. Det är till exempel felaktigt att sekretessbelägga adressinformation för sådana tjänster som är avsedda att vara tillgängliga för allmänheten t.ex. IP-adressen för Försvarsmaktens webbplats.

Uppgifter som lämnar eller kan bidra till upplysning om säkerhetsåtgärder i ett *IT-system* omfattas också av bestämmelsens tredje punkt. Säkerhetsåtgärder behöver inte enbart vara av teknisk natur utan kan även röra administrativa rutiner som utgör en del av säkerhetsåtgärderna i ett IT-system exempelvis rutiner för manuell analys av säkerhetsloggar.

Sekretess för säkerhetsåtgärder gäller oavsett vilka uppgifter som behandlas i ett IT-system eller hur betydelsefullt ett IT-system är för verksamheten. Det är inte enbart de säkerhetsåtgärder som syftar till att säkerställa sekretessen för uppgifterna i ett IT-system som omfattas av sekretess. Även de säkerhetsåtgärder som säkerställer tillgänglighet i ett IT-system omfattas av sekretess om ett röjande av uppgifterna kan antas motverka syftet med säkerhetsåtgärden. Ytterligare ett exempel är ett IT-system som är avsett för offentliga uppgifter och som behöver skyddas mot obehörig ändring t.ex. Försvarsmaktens webbplats. Sekretessbestämmelsen kan således avse andra säkerhetsåtgärder än de som ska säkerställa sekretessen för uppgifter i ett IT-system.

3.4.4 Behörighet i IT-system

Säkerhets- och bevakningssekretessens fjärde punkt behandlar arrangemang och fördelning av behörighetskoder och behörighetsnycklar. Detta kan exempelvis omfatta användarens och administratörers lösenord till IT-system, personliga koder till aktiva kort eller s.k. privata nycklar för autentisering. Även lösenord till utrustning som ingår i IT-system och som ordinarie användare normalt inte har åtkomst till (kommunikationsutrustning) omfattas av sekretessen. Användarnamn för autentisering i IT-system omfattas normalt inte av sekretessbestämmelsen.

3.4.5 Rätten att meddela och offentliggöra uppgifter

För uppgifter som omfattas av sekretess enligt bestämmelsen om säkerhets- och bevakningssekretess gäller tystnadsplikt, som inskränker rätten att meddela och offentliggöra uppgifter. Det innebär att det inte råder någon rätt för den enskilde att meddela och offentliggöra sådana uppgifter. I detta fall råder det alltså ingen meddelarfrihet.⁴⁰ Se även avsnitt 2.2.4.

3.5 Upphandlingssekretess

Sekretess gäller för uppgift som hänför sig till ärende om förvärv, överlåtelse, upplåtelse eller användning av egendom, tjänst eller annan nyttighet, om det kan antas att det allmänna lider skada om uppgiften röjs.

Om ett ärende enligt första stycket rör upphandling, får uppgift som rör anbud eller som rör motsvarande erbjudande inom en kommun, ett landsting eller en myndighet eller mellan statliga myndigheter inte i något fall lämnas till någon annan än den som har lämnat anbudet eller erbjudandet förrän alla anbud eller erbjudanden offentliggörs eller beslut om leverantör och anbud fattats eller ärendet dessförinnan har slutförts.

Om ett ärende enligt första stycket rör försäljning av lös egendom för det allmännas räkning, får uppgift som rör anbud eller som rör motsvarande erbjudande inom en kommun, ett landsting eller en myndighet eller mellan statliga myndigheter inte i något fall lämnas till någon annan än den som har lämnat anbudet eller erbjudandet förrän alla anbud eller erbjudanden offentliggörs eller avtal har slutits eller ärendet annars slutförts.

För uppgift i en allmän handling gäller sekretessen i högst tjugo år. Beträffande handling som anger villkoren i slutet avtal gäller sekretessen dock längst till dess två år, eller hos statliga affärsverk och Försvarets materielverk samt i kommunal affärsverksamhet i fem år, har gått från det avtalet slöts.

19 kap. 3 § offentlighets- och sekretesslagen
(utdrag ur bestämmelsen)

3.5.1 Tillämpning av upphandlingssekretes

I paragrafen regleras den s.k. upphandlingssekretessen. Enligt första meningen gäller sekretess för uppgifter som hänför sig till vissa typer av ärenden. Uttrycket ”*uppgifter som hänför sig till*” innebär att sekretessen följer med uppgifterna när de lämnas till en annan myndighet. De ärenden som avses i bestämmelsen gäller förvärv (t.ex. köp, byte eller gåva), överlåtelse, upplåtelse eller användning av egendom, tjänst eller annan nyttighet. Även uppgifter i ärenden som inte avser t.ex. en konkret försäljning utan en mera inledande kartläggning av möjligheter till en framtida försäljning kan omfattas av upphandlingssekretess.

Paragrafen tar främst sikte på upphandlings- och entreprenadärenden. Det finns ett betydande intresse av insyn i myndigheternas handläggning av det

slag av ärenden som avses i denna bestämmelse. Mot detta står att insynen inte får sträcka sig så långt att det allmänna p.g.a. detta skulle lida ekonomisk skada. Ett exempel på sådan skada är att myndighetens ställning i förhandlingar på grundval av anbudet kan försvagas eller att kommande anbuds-förfarande påverkas negativt av att uppgifter lämnas ut.

I paragrafens andra och tredje stycken finns särskilda regler om sekretess kring anbuds-förfaranden som angår upphandling respektive försäljning av lös egendom för det allmännas räkning. I sådana ärenden får uppgifter som rör ett anbud inte lämnas ut annat än till den som har lämnat anbudet. Sekretessen är med andra ord absolut under den normalt korta tid den gäller. Till uppgifter som rör anbud hör uppgifter som kan tjäna som upplysning, om ett visst anbud har krävts in eller avgetts, eller som på annat sätt avser ett visst anbud, häri inbegrips arbetspromemorior och andra handlingar som har upprättats av myndigheten, t.ex. egna motförslag i samband med en förhandling vid upphandlingsförhandling.

Den absoluta sekretessen gäller till dess ett avtal har slutits eller ärendet annars har slutförts. Denna sekretess upphör dessförinnan, om s.k. offentlig anbudsöppning tillämpas. Alla anbud och motsvarande erbjudande blir då offentliga på en gång. Naturligt nog gäller den absoluta sekretessen för uppgifter som rör ett visst anbud inte gentemot den som har lämnat anbudet.

Bestämmelsen om upphandlingssekretess skyddar bara det allmännas ekonomiska intresse. Sådan sekretess i en myndighets affärsförbindelse som gäller till skydd för en enskild, exempelvis en avtalspart regleras i 31 kap. 16 § OSL s.k. affärssekretess, se kommande avsnitt.

Uppgifter som omfattas av upphandlingssekretess utgör alltid *sekretessklassificerade* uppgifter.

3.5.2 Konsulter

Den absoluta sekretessen för uppgifter som rör ett anbud eller annat erbjudande hindrar inte att uppgifterna exempelvis lämnas ut till en utanför myndigheten stående konsult som behöver dessa uppgifter för att lösa ett uppdrag för myndighetens räkning. En konsult kan i många fall anses delta i myndighetens verksamhet på ett sådant sätt att han eller hon får sägas ingå i myndigheten. Grunden för ett sådant utlämnande finns i 10 kap. 2 § OSL. Det är dock inte säkert att OSL-bestämmelser om sekretess kommer att bli bindande för konsulten. I sådana fall är det därför av vikt att i det affärsmässiga avtal som finns med konsulten eller med konsultens arbetsgivare ta in särskilda föreskrifter om sekretess. I vissa fall kan dock en konsults verksamhet

vara sådan att han eller hon anses vara en osjälvständig uppdragstagare och att OSL bestämmelser blir tillämpliga för denne.

3.5.3 Rätten att meddela och offentliggöra uppgifter

Rätten att meddela uppgifter för offentliggörande, och offentliggöra uppgifter, i tryckt skrift eller i vissa andra medier, d.v.s. den s.k. meddelarfriheten regleras i tryckfrihetsförordningen⁴¹ (TF) och i yttrandefrihetsgrundlagen⁴² (YGL). För uppgifter som omfattas av bestämmelsen om upphandlingssekretess gäller meddelarfrihet. Se även avsnitt 2.2.4.

3.6 Affärssekretess

Secretess gäller för uppgift om en enskilds affärs- eller driftförhållanden när denne i annat fall än som avses i 1 § första stycket, 2-4 och 12 § har trätt i affärsförbindelse med en myndighet, om det av särskild anledning kan antas att den enskilde lider skada om uppgiften röjs.

För uppgifter i en allmän handling gäller sekretessen i högst tjugo år. Beträffande handling som anger villkoren i ett avtal gäller sekretessen dock längst till dess att två år, eller hos statliga affärsverk och Försvarets materielverk samt i kommunal affärsverksamhet fem år, har gått från det att avtalet slöts.

31 kap. 16 § offentlighets- och sekretesslagen

3.6.1 Tillämpning av affärssekretess

Bestämmelsen om affärssekretess ger skydd åt en enskild som har trätt i affärsförbindelse med en myndighet. Det som skyddas är uppgifter om den enskildes affärs- och driftförhållanden. En affärsförbindelse kan exempelvis gälla köp, försäljning, eller upplåtelse av egendom eller arbete som ska utföras. Vid bedömningen om affärssekretess är tillämpligt eller inte, ska man alltid göra en avvägning med hänsyn till offentlighetsintresset. Bestämmelsen om affärssekretess är utformad med ett rakt skaderekvisit. Detta innebär att offentlighet gäller som huvudregel för en uppgift, men att det ska göras en prövning där det av *särskild anledning* ska kunna antas att ett röjande av uppgiften leder till att den enskilde lider skada.

Uppgifter som omfattas av affärssekretess utgör alltid *sekretessklassificerade* uppgifter.

3.6.2 Sekretesstiden

Sekretesstiden för uppgifter i allmänna handlingar är högst 20 år. Beträffande handlingar som anger villkoren i ett slutet avtal gäller sekretessen dock hos bl.a. Forsvarsmakten högst två år eller hos de statliga affärsverken och hos Forsvarets materielverk högst fem år från det att avtalet slöts. Om Forsvarsmakten förvarar en handling från t.ex. FMV för vilken sekretess enligt nyssnämnda bestämmelse gäller överförs sekretessen, enligt 31 kap. 18 § OSL, till Forsvarsmakten, vilket får till följd att även sekretesstiden (högst fem år) överförs.

3.6.3 Rätten att meddela och offentliggöra uppgifter

Rätten att meddela uppgifter för offentliggörande, och offentliggöra uppgifter, i tryckt skrift eller i vissa andra medier, d.v.s. den s.k. meddelarfriheten regleras i TF⁴³ och i YGL.⁴⁴ För uppgifter som omfattas av bestämmelsen om affärssekretess gäller meddelarfrihet. Se även avsnitt 2.2.4.

4 Informationssäkerhetsklasser

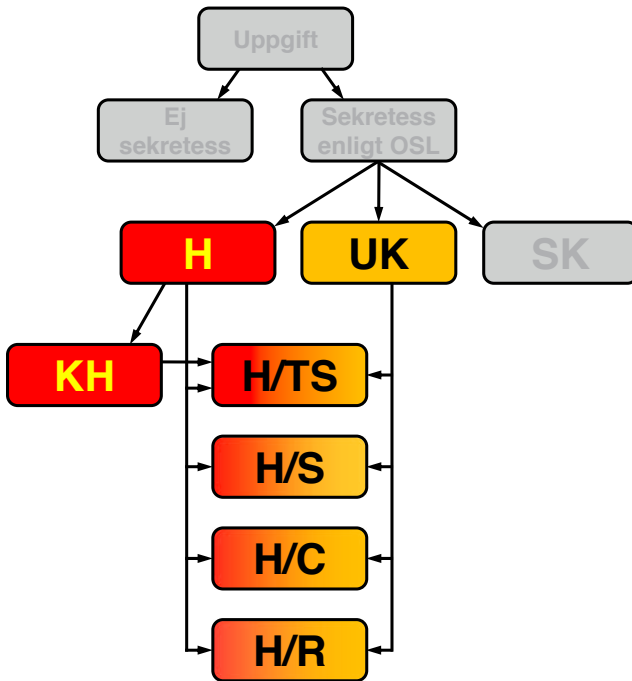


Bild 4.1

4.1 Inledning

Uppgifter vilka efter sekretessbedömning (se kapitel 3) konstaterats vara hemliga eller utrikesklassificerade ska placeras i informationssäkerhetsklass.

I detta kapitel beskrivs informationssäkerhetsklasserna samt hur vissa uppgifter som omfattas av sekretess bedöms och placeras i rätt informationssäkerhetsklass. Syftet med detta kapitel är att ge stöd vid placering av dessa uppgifter i rätt informationssäkerhetsklass.

4.2 Informationssäkerhetsklasser

Säkerhetsskyddet i Försvarsmakten, samt i de myndigheter för vilka Försvarsmakten har föreskriftsrätt över, är indelat i fyra informationssäkerhetsklasser. Informationssäkerhetsklass är en beteckning som anger hur uppgifter ska hanteras för att ett tillräckligt säkerhetsskydd ska erhållas. En informationssäkerhetsklass anger inte sekretessen för en uppgift eller handling utan enbart hur uppgiften eller handlingen ska *hanteras* för att erhålla rätt

skyddsnivå. Informationssäkerhetsklasserna är indelade i nivåerna HEMLIG/TOP SECRET, HEMLIG/SECRET, HEMLIG/CONFIDENTIAL och HEMLIG/RESTRICTED. En högre informationssäkerhetsklass (t.ex. HEMLIG/TOP SECRET) innebär ett starkare skydd jämfört med en lägre informationssäkerhetsklass (t.ex. HEMLIG/SECRET). Med ovanstående indelning ges olika uppgifter som är placerade i skilda informationssäkerhetsklasser ett balanserat säkerhetsskydd med hänsyn till uppgiftens betydelse. Placeringen av uppgifter i informationssäkerhetsklass får inte ske med utgångspunkt från de kostnader som är förenade med skyddet.

Hemliga uppgifter ska placeras i informationssäkerhetsklass på grund av att uppgifterna omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400), nedan OSL, och rör rikets säkerhet. Hemliga uppgifter ska enligt säkerhetsskyddslagen (1996:627) ges ett säkerhetsskydd.

Utrikesklassificerade uppgifter ska också placeras i informationssäkerhetsklass. För att stärka skyddet för utrikesklassificerade uppgifter har Försvarsmakten beslutat Försvarsmaktens föreskrifter (FFS 2010:1) om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar. I enlighet med dessa föreskrifter ska en utrikesklassificerad uppgift eller handling ha ett skydd som motsvarar vad som gäller för en hemlig uppgift och handling enligt Försvarsmaktens föreskrifter (FFS 2003:7) om säkerhetsskydd samt Försvarsmaktens interna bestämmelser (FIB 2007:2) om säkerhetsskydd och skydd av viss materiel.⁴⁵ Utrikesklassificerade uppgifter och handlingar ska därför placeras i informationssäkerhetsklass. Försvarsmakten upprättar utrikesklassificerade handlingar främst vid internationellt samarbete, t.ex. inom ramen för en EU- eller NATO-operation.

En handling som har försetts med en motsvarighet till informationssäkerhetsklass av en utländsk myndighet eller mellanfolklig organisation kan även vara av betydelse för rikets säkerhet och därmed hemlig. I sådana fall uppstår ett *men* för totalförsvaret eller förhållandet till en annan stat eller en mellanfolklig organisation eller i annat fall för rikets säkerhet, om uppgiften röjs.

I Försvarsmakten och vid de myndigheter för vilka Försvarsmakten föreskriver om säkerhetsskydd, indelas säkerhetsskyddet i fyra informationssäkerhetsklasser med följande beteckningar, betydelser och konsekvensbeskrivningar.⁴⁶

Informations- säkerhetsklass	Betydelse	Konsekvens- beskrivning
<i>HEMLIG/TOP SECRET</i>	<p>1. Hemliga uppgifter vars röjande kan medföra synnerligt men för totalförsvaret eller förhållandet till en annan stat eller en mellanfolklig organisation eller i annat fall för rikets säkerhet.</p> <p>2. Hemlig handling som har försetts med beteckningen TOP SECRET eller motsvarande av en utländsk myndighet eller mellanfolklig organisation.</p>	<p>Förväntade konsekvenser medför en synnerlig negativ effekt. Konsekvenserna innebär synnerligen allvarliga negativa effekter av stor omfattning, under lång tid och utgör ett direkt hot mot organisationen.</p> <p>Konsekvenserna är inte begränsade till enstaka förmågor eller funktioner inom organisationen.</p>
<i>HEMLIG/SECRET</i>	<p>1. Hemliga uppgifter vars röjande kan medföra betydande men för totalförsvaret eller förhållandet till en annan stat eller en mellanfolklig organisation eller i annat fall för rikets säkerhet.</p> <p>2. Hemlig handling som har försetts med beteckningen SECRET eller motsvarande av en utländsk myndighet eller mellanfolklig organisation.</p>	<p>Konsekvenserna är allvarliga, av stor omfattning eller av väsentlig art och innebär ett direkt hot, om än mot avgränsade förmågor eller funktioner inom organisationen.</p>

Informations-säkerhetsklass	Betydelse	Konsekvens-beskrivning
<i>HEMLIG/CONFIDENTIAL</i>	<p>1. Hemliga uppgifter vars röjande kan medföra ett inte obetydligt men för totalförsvaret eller förhållandet till en annan stat eller en mellanfolklig organisation eller i annat fall för rikets säkerhet.</p> <p>2. Hemlig handling som har försetts med beteckningen CONFIDENTIAL eller motsvarande av en utländsk myndighet eller mellanfolklig organisation.</p>	<p>Förväntade konsekvenser är inte obetydliga och äventyrar, vållar skada, hindrar, underlättar, innebär större avbrott samt medför påtagliga negativa effekter om än i begränsad omfattning.</p>
<i>HEMLIG/RESTRICTED</i>	<p>1. Hemliga uppgifter vars röjande kan medföra endast ringa men för totalförsvaret eller förhållandet till en annan stat eller en mellanfolklig organisation eller i annat fall för rikets säkerhet.</p> <p>2. Hemlig handling som har försetts med beteckningen RESTRICTED eller motsvarande av en utländsk myndighet eller mellanfolklig organisation.</p>	<p>Förväntade konsekvenser är ringa och begränsas till att påverka, försvåra, hindra, undergräva, misskreditera eller störa verksamheten i mindre omfattning.</p>

Tabell 4.1

4.3 Placering av hemliga uppgifter i informationssäkerhetsklass

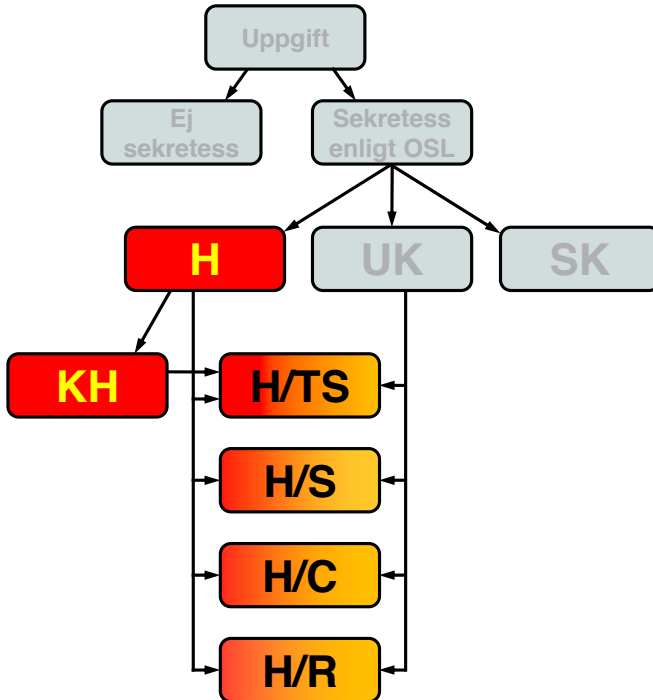


Bild 4.2

4.3.1 Inledning

Placering av hemliga uppgifter i informationssäkerhetsklass styrs av det *men* som uppstår för totalförsvaret eller förhållandet till en annan stat eller en mellanfolklig organisation eller i annat fall för rikets säkerhet, om en hemlig uppgift röjs. Metoden för placering av hemliga uppgifter i informationssäkerhetsklass genomförs som en förtida menbedömning.

4.3.2 Förtida menbedömning

Inledningsvis bedöms de konsekvenser ett eventuellt röjande av uppgifterna skulle få för försvaret eller rikets säkerhet i övrigt. Konsekvenserna klarläggs på ett konkret sätt vilket innebär att det mycket tydligt framgår vari *menet* består. Vad är det för typ av uppgift det handlar om, vilken konsekvens får ett röjande för vår förmåga, vilken funktion är det som påverkas, påverkas den negativt under kort eller lång tid, hur lång tid och vilka resurser kommer att krävas för att reparera skadan (*menet*).

Exempel 4.1

Mycket detaljerade uppgifter om målsökningsfunktionen i en av Försvarsmaktens mest kvalificerade sjömålsrobotar har efter en inledande sekretessbedömning bedömts kunna skada totalförsvaret eller rikets säkerhet i övrigt om de röjs. Uppgifterna är därför hemliga (omfattas av sekretess enligt 15 kap. 2 § OSL och rör rikets säkerhet).

Om en motståndare får tillgång till uppgifterna kan varnings- och motmedelssystem utvecklas. Vidare kan uppgifterna ligga till grund för en taktikanpassning från motståndarens sida. Åtgärderna bedöms resultera i att vår förmåga att bekämpa fiendliga fartyg nedgår med minst hälften. Detta innebär för motståndarens del att sannolikheten för att lyckas med t.ex. en landstigningsoperation ökar högst avsevärt. Konsekvenserna för Försvarsmakten blir att vår förmåga att möta fiendliga sjöoperationer allvarligt försämras.

Den genomförda konsekvensbedömningen av ett röjande vägs sedan mot konsekvensbeskrivningen i tabell 4.1.

Förväntade konsekvenser av att detaljerade uppgifter om målsökningsfunktionen för en av våra mest kvalificerade sjömålsrobotar röjs bedöms vara mycket allvarliga för vår sjöoperativa förmåga och innebär ett direkt hot, om än mot avgränsade förmågor eller funktioner inom Försvarsmakten. Uppgifterna placeras därför, med stöd av tabell 4.1, i informationssäkerhetsklass HEMLIG/SECRET.

Observera att detta endast är ett exempel för att påvisa metodiken vid placering av hemliga uppgifter i informationssäkerhetsklass. Uppgifterna i exemplet skulle beroende på konsekvenser kunna vara placerade i såväl en lägre som högre informationssäkerhetsklass.

Vid placering av hemliga uppgifter i informationssäkerhetsklass är det viktigt att den som gör bedömningen har erforderlig sakkunskap. Utan sådan sakkunskap kan konsekvenser inte bedömas på ett konkret och korrekt sätt.

I en handling är det vanligt att det förekommer flera hemliga uppgifter. I sådant fall är det den uppgift vilken om den röjs orsakar störst *men* som styr placeringen i informationssäkerhetsklass.

4.3.3 Informationssäkerhetsklassen HEMLIG/TOP SECRET

En uppgift som omfattas av sekretess enligt OSL och som rör rikets säkerhet och som dessutom är av synnerlig betydelse för rikets säkerhet benämns *kvalificerat hemlig* (KH). En kvalificerat hemlig uppgift placeras i informationssäkerhetsklass HEMLIG/ TOP SECRET.

En *hemlig* handling som inkommer från en annan stat eller mellanfolklig organisation och som har åsatts beteckningen TOP SECRET eller motsvarande ska placeras i informationssäkerhetsklass HEMLIG/TOP SECRET (t.ex. en handling från EU märkt TRÈS SECRET UE/EU TOP SECRET och som rör rikets säkerhet). En sådan handling behöver inte vara av synnerlig betydelse för rikets säkerhet varför den i sådana fall inte är *kvalificerat hemlig*.

4.3.4 Aggregation

I de fall flera hemliga uppgifter finns i en handling måste det även ske en bedömning av om den sammantagna konsekvensen av att flera uppgifter röjs överstiger konsekvensen för en enskild uppgift. Exempelvis kan en handling innehålla uppgifter vilka enskilt bedöms vara placerade i informationssäkerhetsklass HEMLIG/RESTRICTED. Om samtliga uppgifter i handlingen röjs medför det ett större men än ringa, varför handlingen i sin helhet ska placeras i en högre informationssäkerhetsklass. På motsvarande sätt ska aggregation av uppgifter uppmärksammas i en säkerhetsanalys inför utveckling av ett IT-system.⁴⁷ Aggregation av uppgifter med avseende på placering i informationssäkerhetsklass kan delas in i tre fall.

1. *Varken mängd eller kombination av uppgifter förändrar placering i informationssäkerhetsklass.* Placering i informationssäkerhetsklass av informationsmängden är densamma som den högsta informationssäkerhetsklass som någon av uppgifterna har placerats i. Även om hela eller delar av den samlade mängden uppgifter röjs, går det inte att ur informationsmängden skapa nya uppgifter som hade resulterat i placering i en högre informationssäkerhetsklass. Ett röjande av hela eller delar av den samlade mängden uppgifter resulterar därmed inte i en högre grad av men (se bild 4.3).

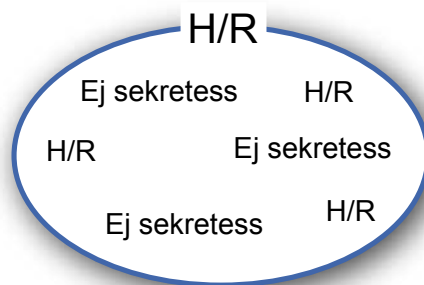


Bild 4.3

2. *Genom att kombinera flera uppgifter erhålls nya uppgifter som inte hade varit möjlig att erhålla med tillgång endast till uppgifterna var och en för sig.* I detta fall är det inte mängden uppgifter som gör att placering i informationssäkerhetsklass förändras utan innehållet i de nya uppgifterna i sig. Ett röjande av hela eller delar av den samlade mängden uppgifter resulterar därmed i en högre grad av men. De nya uppgifterna som kan erhållas genom att kombinera olika specifika uppgifter förändrar därmed placering i informationssäkerhetsklass. Placering i informationssäkerhetsklass för informationsmängden är därmed densamma som den högsta informationssäkerhetsklass

som någon av de kombinerade uppgifterna har placerats i (se bild 4.4). Att konstatera att en kombination av uppgifter i ett IT-system på detta sätt inte resulterar i placering i en högre informationssäkerhetsklass sker i en säkerhetsanalys.

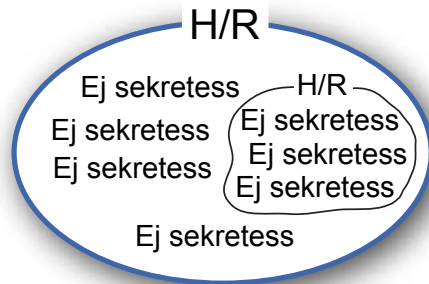


Bild 4.4

3. *Mängden uppgifter förändrar placering i informationssäkerhetsklass.* Ett röjande av hela eller delar av den samlade mängden uppgifter bedöms innebära ett men som är högre än menet vid ett röjande av varje enskild uppgift för sig. Den samlade informationsmängden placeras därför i en högre informationssäkerhetsklass än de enskilda uppgifterna (se bild 4.5).

Detta fall bedöms vara vanligast i fråga om IT-system.

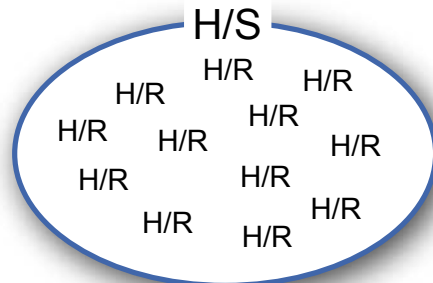


Bild 4.5

4.4 Placering av utrikesklassificerade uppgifter i informationssäkerhetsklass

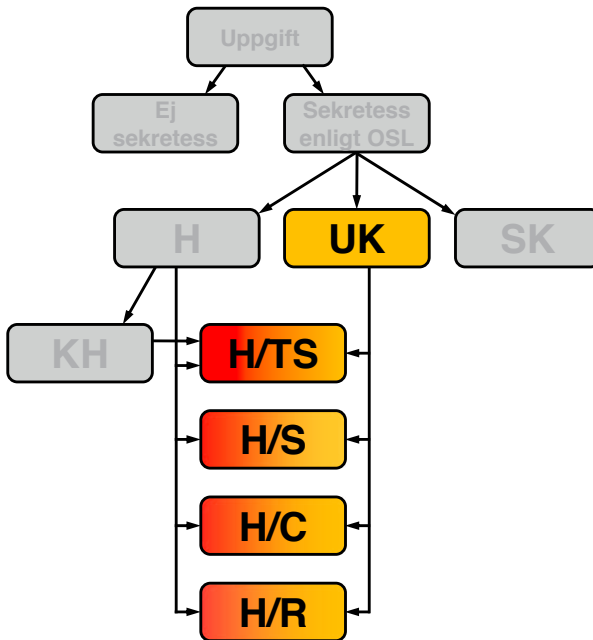


Bild 4.6

4.4.1 Inledning

En utrikesklassificerad uppgift är en uppgift som av en utländsk myndighet eller mellanfolklig organisation eller av en svensk myndighet har klassificerats i någon av nivåerna TOP SECRET, SECRET, CONFIDENTIAL eller RESTRICTED eller motsvarande och som omfattas av sekretess enligt 15 kap. 1 § OSL men som *inte* rör rikets säkerhet.⁴⁸ Utrikesklassificerade uppgifter ska placeras i informationssäkerhetsklass.⁴⁹

4.4.2 Inkommen handling

I Försvarmaktens verksamhet är förekomsten av utrikesklassificerade uppgifter vanligast när utrikesklassificerade handlingar inkommer till Försvarmakten och därmed ska placeras i informationssäkerhetsklass. En betydande del av dessa handlingar är upprättade av annan stat eller mellanfolklig organisation och är redan märkt med beteckning som motsvarar en informa-

tionssäkerhetsklass och ska då i enlighet med Försvarmaktens föreskrifter placeras i informationssäkerhetsklass. I bilaga 2 finns en tabell med andra staters och mellanfolkliga organisationers motsvarighet till informationssäkerhetsklasser.

En utrikesklassificerad handling ska alltid föras med svensk informationssäkerhetsklass. Om det är lämpligt eller särskilt avtalat får handlingen även föras med en märkning som motsvarar en informationssäkerhetsklass inom det aktuella samarbetet, t.ex. RESTREINT UE/EU RESTRICTED.

4.4.3 Upprättad handling

Försvarmakten kan även upprätta utrikesklassificerade handlingar. Den verksamhet där det förekommer är t.ex. vid svenskt deltagande i en EU- eller NATO-operation. En handling som upprättas i Försvarmakten och som innehåller uppgift som omfattas av sekretess enligt 15 kap. 1 § OSL kan utgöra en utrikesklassificerad handling. För att detta ska gälla ska uppgiften röra ett internationellt samarbete och uppfylla ett av följande villkor.

- 1) Uppgiften omfattas av en klassningsguide eller andra riktlinjer för placering i motsvarighet till informationssäkerhetsklass för det aktuella internationella samarbetet (se exempel 4.2 nedan).
- 2) Uppgiften skulle ha varit en hemlig uppgift om den hade rört ett motsvarande nationellt förhållande i Sverige. Den ska då placeras i samma informationssäkerhetsklass som om den hade varit en hemlig uppgift (se exempel 4.3 nedan).

Handlingen ska placeras i informationssäkerhetsklass och får även föras med en märkning som motsvarar informationssäkerhetsklass inom det internationella samarbetet, t.ex. RESTREINT UE.

Exempel 4.2

Sverige har ett samarbetsavtal med tre länder avseende ett materielprojekt där länderna gemensamt utvecklar en ny typ av sjömålsrobot. Projektet omfattar flera versioner av sjömålsroboten och några av dessa är inte avsedda att användas för försvaret av Sverige. Inom ramen för materielprojektet finns en klassningsguide som beskriver vilka uppgifter om sjömålsroboten som ska placeras i informationssäkerhetsklass. De uppgifter i projektet som inte rör försvaret av Sverige omfattas av utrikessekretess och utgör utrikesklassificerade uppgifter eftersom uppgifterna omfattas av ett internationellt åtagande om skydd för uppgifterna. Uppgifterna om den version som ska användas för försvaret av Sverige omfattas av försvarssekretess och utgör därmed hemliga uppgifter.

Exempel 4.3

Inom ramen för Sveriges och Försvarsmaktens deltagande i den NATO-ledda operationen i Afghanistan upprättas en operationsplan för en kommande säkerhetsoperation i det svenska ansvarsområdet. Eftersom ett röjande av operationsplanen skulle kunna antas skada Sveriges relationer med NATO omfattas planen av utrikessekretess. Handlingen omfattas av ett internationellt säkerhetsskyddsåtagande och utgör därför en utrikesklassificerad handling. Eftersom motsvarande operationsplan för försvaret av Sverige skulle ha varit en hemlig handling och placerats i informationssäkerhetsklassen HEMLIG/SECRET ska även den svenska operationsplanen i den NATO-ledda operationen placeras i informationssäkerhetsklass HEMLIG/SECRET.

5 Utlämnande av allmänna handlingar

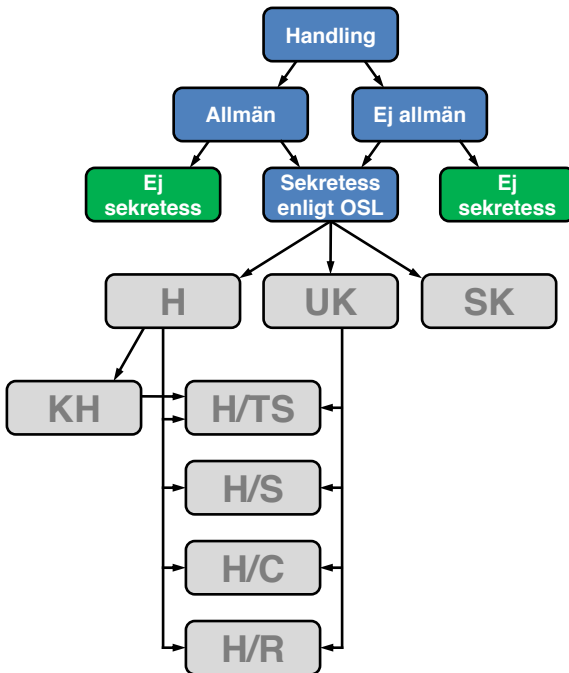


Bild 5.1

5.1 Bakgrund

Syftet med detta kapitel är att utgöra ett stöd för den som ska pröva frågan om utlämnande av en allmän handling.

5.2 Skyndsam handläggning

Frågan om utlämnande av en allmän handling ska prövas skyndsamt.⁵⁰ Ett beslut bör helst meddelas samma dag, men någon dags fördröjning kan beroende på materialets karaktär och omfång accepteras för att bereda myndigheten rådrom att ta ställning till om handlingen kan lämnas ut. I vissa fall kan komplicerade eller omfattande ärenden ta längre tid i anspråk för att sekretessfrågan ska kunna avgöras på ett korrekt sätt. Även i dessa fall gäller dock skyndsamhetskravet.

5.3 Anonymitet

Vem som helst, svensk eller utländsk medborgare, har rätt att ta del av allmänna handlingar. En myndighet har inte rätt att efterforska varför personen vill ha vissa handlingar eller vad han eller hon heter.

5.4 Handläggningen av utlämningsärenden i Försvarsmakten

Beträffande utlämnande av allmänna handlingar till en enskild framgår det av 23 § förordningen (2007:1266) med instruktion för Försvarsmakten att organisationsenhet ska pröva frågor om utlämning av allmänna handlingar som förvaras vid organisationsenheten. I tveksamma fall eller om sökanden begär att frågan ska överlämnas till myndigheten ska prövningen göras av chef för organisationsenheten. När det gäller handlingar som förvaras i Högkvarteret ska frågan i stället prövas av chefen för den enhet som överbefälhavaren har beslutat. I Försvarsmaktens arbetsordning framgår det att det är chefen för juridiska staben som ansvarar för att på myndighetens vägnar fatta beslut i sådana ärenden.⁵¹

En chef för en organisationsenhet har dock rätt att begära stöd av chefen för juridiska staben vid Försvarsmaktens högkvarter när det gäller prövning av en handling som förvaras på organisationsenheten. Detta finns reglerat 23 § förordningen (2007:1266) med instruktion för Försvarsmakten respektive i 13 kap. 10 § Försvarsmaktens föreskrifter (FFS 2010:9) med arbetsordning för Försvarsmakten (FM ArbO).

Om ett beslut innebär att handlingen inte lämnas ut eller inskränker den enskildes rätt att röja innehållet eller på annat sätt förfoga över handlingen, ska den enskilde upplysas om möjligheten att begära myndighetens prövning och att det krävs ett skriftligt beslut av myndigheten för att beslutet ska kunna överklagas. I praktiken utformas besluten direkt som sådana, av myndigheten fattade, avslagsbeslut. Beslutet ska därmed innehålla en upplysning till den enskilde om hur beslutet kan överklagas.

I bilaga 1 finns ett exempel på hur ett avslagsbeslut kan vara utformat.

5.5 Sekretessgranskning

Vid en prövning av om en allmän handling kan lämnas ut måste man först bedöma om handlingen är en allmän handling eller inte. Grunderna för allmänna handlingar beskrivs ovan i kapitel 2.1.3. Om handlingen inte är en allmän handling behöver den inte lämnas ut. Detta gäller t.ex. om handlingen inte längre förvaras vid myndigheten. I dessa fall måste myndigheten fatta ett beslut med detta innehåll och med tillämplig anvisning om hur man överklagar.

När det har konstaterats att den handling som ska prövas är en allmän handling, ska sekretessfrågan bedömas. En sekretessmarkering utgör i sig inte något hinder mot ett utlämnande, men den utgör en varningssignal att handlingen *kan* innehålla uppgifter som omfattas av sekretess. Observera att handlingen även kan innehålla uppgifter som omfattas av annan sekretess än den som anges i märkningen. Ibland kan frågan om sekretess vara enkel att avgöra medan det ibland behövs specifik kompetens avseende det ämnesområde som handlingen rör. Vid komplicerade bedömningar har naturligtvis myndigheten eller organisationsenheten en viss tid för rådrum, men denna typ av ärenden är prioriterade och ska därför handläggas skyndsamt.

Efter det att sekretessen har bedömts måste *sekretesstiden* beaktas. De flesta uppgifter som omfattas av sekretess har en maxtid för hur länge sekretess kan gälla för uppgifterna, när de förekommer i en allmän handling. Om maxtiden har överskridits gäller inte längre sekretess för uppgifterna.

5.6 Förbehåll

Om en myndighet finner att sådan risk för skada, men eller annan olägenhet som enligt en bestämmelse om sekretess hindrar att en uppgift lämnas till en enskild kan undanröjas genom ett förbehåll som inskränker den enskildes rätt att lämna uppgiften vidare eller utnyttja den, ska myndigheten göra ett sådant förbehåll när uppgiften lämnas till den enskilde.

10 kap. 14 § offentlighets- och sekretesslagen
(utdrag ur bestämmelsen)

I 10 kap. 14 § offentlighets- och sekretesslagen (OSL) finns bestämmelser om förbehåll vid utlämnande av uppgifter till enskilda. Förbehåll kan endast tillämpas i en situation där uppgifter som omfattas av sekretess ska kunna lämnas ut till en sökande. Det kan vara angeläget att göra detta exempelvis när en forskare vill ta del av äldre handlingar. Det innebär att Försvarsmakten i samband med utlämning av en handling kan uppställa vissa villkor för den enskilde i samband med utlämning av en handling.

Ett förbehåll kan t.ex. gälla förbud mot vidare spridning av handlingens innehåll som omfattas av sekretess. Genom ett förbehåll uppstår en tystnadsplikt för den enskilde och om han eller hon bryter mot denna gör han eller hon sig skyldig till brott mot tystnadsplikten.⁵²

Ett beslut som innebär att ett förbehåll ställs upp kan överklagas av den enskilde på samma sätt som vid avslagsbeslut.

Bilaga 1 - Exempel på avslagsbeslut vid utlämnande av allmän handling



FÖRSVARSMAKTEN
HÖGKVARTERET

Datum
2011-01-14

HKV beteckning
10 816:12345

Sida 1 (2)

NN
och sändlista

Ert tjänsteställe, handläggare

Ert datum
2011-01-11

Er beteckning

Vårt tjänsteställe, handläggare
HKV MUST

Vårt föregående datum

Vår föregående beteckning

Beslut om utlämnande av handlingar

(1 bilaga)

Framställan

I en framställan via e-post till Försvarsmaktens högkvarter (Högkvarteret) den 11 januari 2011 begär du att få ta del av handlingar som berör följande fyra händelser vid den svenska styrkan i Afghanistan:

- Attacken mot en svensk patrull vecka 940,
- Händelserna i Maimana vecka 940,
- Eldstriden i byn Boka vecka 950 och
- Eldstriden i byn Stin vecka 950.

Myndighetens bedömning

Vid Högkvarteret, Militära underrättelse- och säkerhetstjänsten (MUST), finns ett antal handlingar upprättade från den tid de efterfrågade händelserna inträffade.

Handlingarna har följande beteckning:

- Särskild underrättelserapport, 2009-XX-XX, beteckning H/S XXX/XXX
- Underrättelserapport 2009-XX-XX, beteckning H/S XXX/XXX
- Underrättelserapport 2009-XX-XX, beteckning H/S XXX/XXX
- MUST Lägesbild vecka 940, beteckning H/S XXX/XXX
- MUST Lägesbild vecka 950, beteckning H/S XXX/XXX

När det gäller handlingar som är benämnda MUST Lägesbild består de av tre bilagor. I handlingarna är det bilaga tre som beskriver läget i Afghanistan. Eftersom myndigheten har uppfattat att du i din framställan endast frågar efter uppgifter som berör fyra specifikt angivna händelser i Afghanistan, har myndigheten endast granskat dessa bilagor.

Postadress
107 85 STOCKHOLM

Besöksadress
Lidingövägen 24

Telefon
08-788 75 00

Telefax
08-788 77 78

E-post, Internet
exp-hkv@mil.se
www.hkv.mil.se

FÖRSVARSMAKTEN

HÖGKVARTERET

Datum
2011-01-14HKV beteckning
10 816:12345

Sida 2 (2)

Handlingarna innehåller underrättelsebedömningar och säkerhetshotanalyser. I samtliga handlingar förekommer uppgifter som ger information om den militära underrättelsetjänstens källor och arbetsmetoder. Vidare förekommer uppgifter avseende vissa svenska förbands komponenters taktiska uppträdande och potentiella sårbarhet. Då det kan antas att det skadar landets försvar om dessa uppgifter röjs, omfattas de av sekretess enligt 15 kap. 2 § offentlighets- och sekretesslagen (2009:400).

Till del baseras underlaget i handlingarna även på information som erhållits inom ramen för vårt deltagande i en internationell insats. I vissa handlingar förekommer uppgifter och bedömningar om förhållanden som rör andra stater. Eftersom det kan antas att ett röjande av dessa uppgifter kan störa Sveriges mellanfolkliga förbindelser eller på annat sätt skada landet, omfattas de av sekretess enligt 15 kap. 1 § offentlighets- och sekretesslagen.

Hinder mot att lämna ut ovan nämnda uppgifter föreligger därför. Övriga uppgifter i handlingarna omfattas inte av sekretess och ska lämnas ut.

Med anledning härav meddelar Högkvarteret följande.

BESLUT

Din begäran avslås ifråga om de uppgifter i handlingarna som omfattas av sekretess enligt 15 kap. 1 respektive 2 §§ offentlighets- och sekretesslagen. Din framställan bifalls i fråga om övriga uppgifter i handlingarna. Handlingarna lämnas ut i den omfattning som framgår av bilagan i detta beslut. /1

Hur man överklagar

Detta beslut får överklagas hos Kammarrätten i Stockholm. Överklagandet ska vara skriftligt. I skrivelsen ska anges vilket beslut som överklagas och den ändring som du vill ha. Skrivelsen med överklagandet ska vara ställd till Kammarrätten i Stockholm men skickas till Försvarsmakten, Högkvarteret. Den ska ha kommit in till Försvarsmakten inom tre (3) veckor från den dag du fick del av beslutet.

Beslut i detta ärende har fattats av chefsjurist Stefan Ryding-Berg. I ärendets slutliga handläggning har dessutom deltagit försvarsjurist Olof Göransson, avdelningsdirektör Werner Martinsson och, som föredragande, byrådirektör Katharina Strömhammar.

Stefan Ryding-Berg
Chef för juridiska staben

Katharina Strömhammar

Bilaga 2 - Andra stater och mellanfolkliga organisationers motsvarighet till informationssäkerhetsklasser

STAT/ ORGANISATION	HEMLIG/ TOP SECRET	HEMLIG/ SECRET	HEMLIG/ CONFIDENTIAL	HEMLIG/ RESTRICTED
Belgien	Très Secret	Secret	Confidentiel	Diffusion restreinte
	Zeer geheim	Geheim	Vertrouwelijk	Beperkte verspreiding
Bulgarien	Строго секретно	Секретно	Поверително	За служебно ползване
Cypern	Άκρως Απόρρητο	Απόρρητο	Εμπιστευτικό	Περιορισμένης Χρήσης
Danmark	Yderst hemmeligt	Hemmeligt	Fortroligt	Til tjenestebrug
Estland	Täiesti salajane	Salajane	Konfidentsiaalne	Piiratud
EU	TRÈS SECRET UE/EU TOP SECRET	SECRET UE	CONFIDENTIEL UE	RESTREINT UE
	Förkortas: TS-UE	Förkortas: S-UE	Förkortas: C-UE	Förkortas: R-UE
Euratom	Eura - Top Secret	Eura - Secret	Eura - Confidential	Eura - Restricted
Finland	ERITTÄIN SALAINEN	SALAINEN	LUOTTA-MUKSELLINEN	KÄYTTÖ RAJOITETTU
FN	⁵³			
Frankrike	Très Secret Défense	Secret Défense	Confidentiel Défense	Diffusion Restreinte
Grekland	Άκρως Απόρρητο	Απόρρητο	Εμπιστευτικό	Περιορισμένης Χρήσης
	Förkortas: ΑΑΠ	Förkortas: (ΑΠ)	Förkortas: (ΕΜ)	Förkortas: (ΠΧ)
Irland	Top Secret	Secret	Confidential	Restricted
Italien	Segretissimo	Segreto	Riservatissimo	Riservato
Kanada	Top Secret	Secret	Confidential	Restricted
Lettland	Sevišķi slepeni	Slepeni	Konfidenciāli	Dienesta vajadzībām
Litauen	Visiškai slaptai	Slaptai	Konfidencialiai	Riboto naudojimo
Luxembourg	Très Secret Lux	Secret Lux	Confidentiel Lux	Restreint Lux

STAT/ ORGANISATION	HEMLIG/ TOP SECRET	HEMLIG/ SECRET	HEMLIG/ CONFIDENTIAL	HEMLIG/ RESTRICTED
Malta	L-Ghola Segretezza	Sigriet	Kunfidenzjali	Ristrett
NATO	COSMIC TOP SECRET	NATO SECRET	NATO CONFIDENTIAL	NATO RESTRICTED
	Förkortas: CTS	Förkortas: NS	Förkortas: NC	Förkortas: NR
Nederländerna	STG Zeer geheim	STG Geheim	STG Confidentieel	DEP Vertrouwelijk
Norge	STRENGT HEMMELIG	HEMMELIG	KONFIDENSIELT	BEGRENSET
Polen	Ścisłe Tajne	Tajne	Poufne	Zastrzeżone
Portugal	Muito Secreto	Secreto	Confidencial	Reservado
Rumänen	Strict secret de importanță deosebită	Strict secret	Secret	Secret de serviciu
Schweiz	54	GEHEIM	VERTRAULICH	57
		SECRET	CONFIDENTIEL	
		SEGRETO	CONFIDENZIALE	
Singapore	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
Slovakien	Prísne tajné	Tajné	Dôverné	Vyhradené
Slovenien	Strogo tajno	Tajno	Zaupno	Interno
Spanien	Secreto	Reservado	Confidencial	Difusión Limitada
Storbritannien	UK TOP SECRET	UK SECRET	UK CONFIDENTIAL	UK RESTRICTED
Sydafrika	Top Secret	Secret	Confidential	Restricted
Sydkorea	55	군사 II급 비밀	군사 III급 비밀	군사대외비
		SECRET	CONFIDENTIAL	DAE WOI BI
Tjeckien	Prísne tajné	Tajné	Důvěrné	Vyhrazené
Tyskland	Streng geheim	Geheim	VS – Vertraulich ⁵⁶	VS - Nur für den Dienstgebrauch
Ungern	Szigorúan titkos	Titkos	Bizalmas	Korlátozott terjesztésű
USA	Top Secret	Secret	Confidential	-
WEU ⁵⁸	Focal Top Secret	WEU Secret	WEU Confidential	WEU Restricted
Österrike	Streng Geheim	Geheim	Vertraulich	Eingeschränkt

Bilaga 3 - Råd för formulering

Här anges råd om hur informationsklassificering kan formuleras. Begreppet informationsklassning får användas synonymt med informationsklassificering.

1. Inled med att ange vilken eller vilka sekretessbestämmelser i offentlighets- och sekretesslagen som uppgifterna bedöms omfattas av. Ett lämpligt skrivsätt kan vara ”omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400)”. Begrepp såsom sekretessbelagd eller sekretessreglerad⁵⁹ bör undvikas då begreppen har specifika juridiska betydelser.

ELLER

Om uppgifterna inte omfattas av sekretess anges detta. Ett lämpligt skrivsätt kan då vara ”omfattas inte av sekretess enligt offentlighets- och sekretesslagen (2009:400)”. Benämningar såsom ÖPPEN, UNCLASSIFIED och liknande är inte lämpliga då dessa inte är definierade i Försvarmakten. Benämningen ”EJ SEKRETESS” kan användas som kortform i tabeller, ritningar och liknande. Punkterna 2 till 4 nedan tillämpas inte i de fall uppgifterna inte omfattas av sekretess.

2. Ange om uppgifterna rör rikets säkerhet. Självklart anges detta alltid i fråga om kvalificerat hemliga och hemliga uppgifter. Om uppgifterna är av synnerlig betydelse för rikets säkerhet anges även detta.

ELLER

Ange om uppgifterna inte rör rikets säkerhet. Då uppgifter som omfattas av utrikessekretess kan vara kvalificerat hemliga, hemliga, utrikesklassificerade eller sekretessklassificerade är det nödvändigt att på något sätt ange detta för uppgifter som omfattas av utrikessekretess och som inte rör rikets säkerhet. Det är inte nödvändigt för andra sekretessklassificerade uppgifter.

3. Ange sekretesskategorin som KVALIFICERAT HEMLIG, HEMLIG, UTRIKESKLASSIFICERAD eller SEKRETESSKLASSIFICERAD. Några andra sekretesskategorier finns inte i Försvarmakten. Förkortningarna KH, H, UK och SK får användas i tabeller, ritningar och liknande.
4. Fortsätt informationsklassificeringen med att ange eventuell placering i informationssäkerhetsklass. Ett lämpligt skrivsätt kan vara ”uppgifterna placeras i informationssäkerhetsklass HEMLIG/RESTRICTED”. Sekretessklassificerade uppgifter placeras inte i informationssäkerhetsklass.

Exempel

Nedanstående är exempel som inte är uttömmande.

Exempel: Kvalificerat hemliga uppgifter

Uppgifterna omfattas av sekretess enligt 15 kap. 2 § offentlighets- och sekretesslagen (2009:400). Uppgifterna rör rikets säkerhet och är av synnerlig betydelse för rikets säkerhet. Uppgifterna hör till sekretesskategorin KVALIFICERAT HEMLIG och placeras i informationssäkerhetsklass HEMLIG/TOP SECRET.

Exempel: Hemliga uppgifter

Uppgifterna omfattas av sekretess enligt 15 kap. 2 § offentlighets- och sekretesslagen (2009:400). Uppgifterna rör rikets säkerhet. Uppgifterna hör till sekretesskategorin HEMLIG och placeras i sekretesskategorin HEMLIG/CONFIDENTIAL.

Exempel: Utrikesklassificerade uppgifter

Uppgifterna omfattas av sekretess enligt 15 kap. 1 § offentlighets- och sekretesslagen (2009:400). Uppgifterna rör inte rikets säkerhet. Då uppgifterna omfattas av ett internationellt säkerhetsskyddsåtagande hör uppgifterna till sekretesskategorin UTRIKESKLASSIFICERAD och placeras i informationssäkerhetsklass HEMLIG/SECRET.

Exempel: Sekretessklassificerade uppgifter

Uppgifterna omfattas av sekretess enligt 17 kap. 4 § offentlighets- och sekretesslagen (2009:400). Uppgifterna är SEKRETESSKLASSIFICERADE.

Exempel: Sekretessklassificerade uppgifter

Uppgifterna omfattas av sekretess enligt 15 kap. 1 § offentlighets- och sekretesslagen (2009:400). Uppgifterna rör inte rikets säkerhet och hör till sekretesskategorin SEKRETESSKLASSIFICERADE. Uppgifterna är inte placerade i informationssäkerhetsklass.

Exempel: Ej sekretess

Uppgifterna omfattas inte av sekretess enligt offentlighets- och sekretesslagen (2009:400).

Fotnoter

¹⁴ 4 § säkerhetsskyddsförordningen (1996:633).

²Försvarsmaktens föreskrifter (FFS 2010:1) om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar.

³HKV 2005-04-05, 10 700:65482, Beslut om Försvarsmaktens informationssäkerhetspolicy.

⁴En hemlig uppgift är en uppgift som omfattas av sekretess enligt OSL och som rör rikets säkerhet enligt 4 § säkerhetsskyddsförordningen (1996:633).

⁵2 kap. 2 § Försvarsmaktens föreskrifter (FFS 2003:7) om säkerhetsskydd.

⁶1 kap. 3 § Försvarsmaktens föreskrifter (FFS 2010:1) om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar.

⁷1 kap. 3 § Försvarsmaktens föreskrifter (FFS 2010:1) om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar.

⁸1 kap. 1 § TF.

⁹2 kap. 3 § TF.

¹⁰2 kap. 3 § TF.

¹¹2 kap. 4 § TF.

¹²2 kap. 9 § TF.

¹³3 kap. 1 § OSL.

¹⁴En hemlig handling är en handling som innehåller hemlig uppgift, 4 § säkerhetsskyddsförordningen (1996:633).

¹⁵10 kap. 2 § OSL.

¹⁶8 kap. 3 § OSL.

¹⁷15 kap. 2 § OSL.

¹⁸5 kap. 5 § OSL.

¹⁹HKV 2009-06-26, 10 812:60437, Direktiv om utformning av sekretessmarkering i Försvarsmakten.

²⁰1 kap. 1 § TF och 1 kap. 1 och 2 §§ YGL.

²¹Lag (1993:1742) om skydd för landskapsinformation.

²²Proposition 1996/97:4 s. 54, försvarsutskottets betänkande 1996/97 FöU01 s. 31-32.

²³Proposition 1995/96:129 s. 22.

²⁴4 § offentlighets- och sekretessförordning (2009:641).

²⁵1 kap. 1 § TF.

²⁶1 kap. 1 och 2 §§ YGL.

²⁷7 kap. 3 § TF.

²⁸15 kap. 6 § andra stycket OSL.

²⁹10 kap. 13 § RF.

³⁰Försvarsmaktens föreskrifter (FFS 2010:1) om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar.

³¹Översyn av spioneribrottet m.m., Ds Ju 1979:6 s 26.

³²1 kap. 1 § TF.

³³1 kap. 1 och 2 §§ YGL.

³⁴15 kap. 6 § första stycket OSL.

³⁵Som exempel på teknisk anläggningsdokumentation kan anges ritningar eller placeringsskiss gällande data-, tele- eller elförsörjningssystem för en anläggning.

³⁶Försvarsmaktens föreskrifter (FFS 2010:1) om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar.

³⁷Se kap. 5 Handbok för Försvarsmaktens Säkerhetstjänst, Säkerhetsskyddstjänst (H Säk Skydd 2007).

³⁸13 kap. 4 § brottsbalken.

³⁹4 kap. 8 § brottsbalken.

⁴⁰18 kap. 19 § OSL.

⁴¹1 kap. 1 § TF.

⁴²1 kap. 1 och 2 §§ YGL.

⁴³1 kap. 1 § TF.

⁴⁴1 kap. 1 och 2 §§ YGL.

⁴⁵2 kap. 1 § Försvarsmaktens föreskrifter (FFS 2010:1) om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar.

⁴⁶Handbok för Försvarsmaktens Säkerhetstjänst, Säkerhetsskyddstjänst (H Säk Skydd 2007), s. 44.

⁴⁷7 kap. 8 § Försvarsmaktens föreskrifter (FFS 2003:7) om säkerhetsskydd.

⁴⁸1 kap. 3 § Försvarsmaktens föreskrifter (FFS 2010:1) om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar.

⁴⁹2 kap. 1 § Försvarsmaktens föreskrifter (FFS 2010:1) om skydd för utrikes- och sekretessklassificerade uppgifter och handlingar.

⁵⁰2 kap. 12 § TF.

⁵¹13 kap. 11 § Försvarsmaktens föreskrifter (2010:9) med arbetsordning för Försvarsmakten (FM ArbO).

⁵²20 kap. 3 § brottsbalken.

⁵³FN har ingen officiell motsvarighet till informationssäkerhetsklasser.

⁵⁴Motsvarighet till informationssäkerhetsklass HEMLIG/TOP SECRET ingår inte i avtal med Schweiz (SÖ 2004:5). Information i övrigt saknas.

⁵⁵Motsvarighet till informationssäkerhetsklass HEMLIG/TOP SECRET avses inte ingå i avtal med Sydkorea.

⁵⁶VS är förkortning för Verschlusssache.

⁵⁷Motsvarighet till informationssäkerhetsklassen HEMLIG/RESTRICTED saknas.

⁵⁸Västeuropeiska unionen.

⁵⁹En sekretessreglerad uppgift är en uppgift för vilken det finns en bestämmelse om sekretess, 3 kap. 1 § OSL.

Försvarmakten

Helena Rozi (projektledare)

Martin Waern

Kim Hakkarainen

Ola Areschoug

Mårten Wallén

Anna Svanberg



FÖRSVARSMAKTEN
HÖGKVARTERET