RP 245/2010 rd

Regeringens proposition till Riksdagen om godkännande av det generella säkerhetsskyddsavtalet om ömsesidigt skydd och utbyte av säkerhetsskyddsklassificerade uppgifter mellan Danmark, Finland, Island, Norge och Sverige och med förslag till lag om sättande i kraft av de bestämmelser i avtalet som hör till området för lagstiftningen

PROPOSITIONENS HUVUDSAKLIGA INNEHÅLL

I denna proposition föreslås att riksdagen godkänner det generella säkerhetsskyddsavtalet om ömsesidigt skydd och utbyte av säkerhetsklassificerade uppgifter mellan Danmark, Finland, Island, Norge och Sverige samt lagen om sättande ikraft av de bestämmelser i avtalet som hör till området för lagstiftningen.

Syftet med avtalet är att skydda säkerhetsklassificerade uppgifter som utbyts mellan två eller flera nordiska länder som är fördragsslutande parter, eller mellan kontraktsparter inom de nordiska ländernas jurisdiktion, inom utrikes-, försvars-, säkerhets- och polisärenden eller i vetenskapligt, industriellt eller teknologiskt samarbete, eller som framtagits grundade på eller som härrör från de uppgifter som har utbytts. Det är fråga om särskilt känsligt informationsmaterial som specifikt har klassificerats för en hög säkerhetsnivå i den upprättande fördragsslutande staten.

Avtalet träder i kraft trettio dagar efter det datum då ratifikations-, godtagande- eller godkännandeinstrumenten lämnats in av den sista av de regeringar som har undertecknat avtalet. Fram till att avtalet träder i kraft får varje fördragsslutande part då den lämnar sitt ratifikations-, godtagande- eller godkännandeinstrument eller vid en senare tidpunkt meddela att den anser sig vara bunden av avtalet i förhållande till någon annan fördragsslutande part som har lämnat ett likadant meddelande. Dessa meddelanden träder i kraft trettio dagar efter dagen för mottagandet av meddelandet. Avsikten är att Finland ska lämna ett sådant meddelande. Lagen om sättande i kraft av avtalet avses träda i kraft samtidigt som avtalet träder i kraft vid en tidpunkt som bestäms genom förordning av republikens president.

———

295260

INNEHÅLL

ALLMÄN MOTIVERING

1 Inledning

Med informationssäkerhet avses allmänt taget alla förfaranden som skyddar informationsinnehållet gentemot utomstående (informationens konfidentialitet), informationens oföränderlighet (integritet) samt informationens användbarhet. För att trygga informationssäkerheten används olika metoder. De vanligaste är kontroll av personalens tillförlitlighet och lokalernas säkerhet, sekretessbestämmelser och begränsningar i rätten att använda informationen till enbart överenskommet ändamål, samt olika typer av procedurkrav för hantering och överföring av information. Säkerhetskraven täcker informationens hela livscykel, med andra ord förvärvande, bearbetning, användning, överlåtelse, arkivering och förstöring.

Inom det internationella samarbetet förekommer det handlingar som innehåller sekretessbelagd information som, om den obehörigen röjs, kan medföra betydande och omfattande skada på viktiga allmänna intressen. Denna typ av material måste därför behandlas särskilt omsorgsfullt. Det gäller Finlands trovärdighet som part i det internationella samarbetet.

Det internationella informationssäkerhetssamarbetet, som även Finland är delaktig i, omfattar sedvanligt skydd av ickeoffentligt informationsutbyte som ingår i den diplomatiska verksamheten, liksom även i samarbetet mellan försvars- och polisväsendet. Utöver frågor som lyder under omedelbart statsansvar har internationella förpliktelser som gäller informationssäkerhet också en växande betydelse för det ekonomiska, industriella och teknologiska samarbetet. Allt flera projekt på företagsnivå har kopplingar till klassificerad information. Det här gäller särskilt då det är fråga om myndighetsanskaffningar som förutsätter att sekretessbelagd statlig information lämnas ut till företag för att kommersiella kontrakt ska kunna fullgöras. Traditionellt hör anskaffningar av detta slag särskilt till försvarets område, men sektorn det berör blir allt bredare.

Det har trots olika strävanden inte visat sig vara möjligt att få till stånd en multilateral konvention inom området för informationssäkerhet. Den största orsaken är skillnaderna i nationell lagstiftning samt i administrativa strukturer och kutymer, vilket återspeglar känsligheten i informationssäkerhetsfrågor som en del av den nationella säkerheten överlag.

Bristen på en konvention tvingar således staterna, Finland medräknat, att lösa frågan genom bilaterala avtal. Finland ingick sitt första bilaterala avtal om informationssäkerhet med Tyska förbundsrepubliken år 2004. Det trädde i kraft den 16 juli 2004 (FördrS 96 och 97/2004). Ett år senare undertecknades ett avtal mellan Finland och Frankrike och det trädde i kraft den 1 augusti 2005 (FördrS 66 och 67/2005). Dessa två stora medlemsstater i Europeiska unionen (EU) är viktiga samarbetspartner för Finland, såväl inom området för säkerhetsförvaltning som med tanke på den ekonomiska växelverkan.

Det faktum att behovet av informationssäkerhet i allt högre grad börjar fokusera också på ekonomisk verksamhet kommer till uttryck i samarbetsavtalet mellan Finland och Europeiska rymdorganisationen (ESA), nedan ESA-överenskommelsen, även den från 2004 (FördrS 94 och 95/2004). En av de viktigaste målsättningarna med den överenskommelsen har varit att säkerställa det finländska näringslivets möjligheter att på jämlik grund med de andra medlemsstaterna delta i ESA:s säkerhetsklassificerade anbudsförfaranden. Finland har också ingått ett säkerhetsskyddsavtal med Västeuropeiska unionen VEU (FördrS 41 och 42/1998) och med Organisationen för gemensamt försvarsmaterielsamarbete i Europa OCCAR (FördrS 109 och 110/2008).

Utöver nämnda fördrag har Finland gällande överenskommelser om informationssäkerhet med Slovakien (FördrS 116 och 117/2007), Estland (FördrS 12 och 13/2008), Italien (FördrS 23 och 24/2008), Lettland (FördrS 33 och 34/2008), Polen (FördrS 46 och 47/2008), Bulgarien (FördrS 116 och

117/2008), Slovenien (FördrS 22 och 23/2009), Tjeckien (FördrS 53 och 54/2009) och Spanien (FördrS 38 och 39/2010). Överenskommelserna med Litauen och Nederländerna inväntar undertecknande. Förhandlingar om informationssäkerhetsöverenskommelser är också på gång med Storbritannien, Luxemburg och Schweiz. Också mellan medlemsstaterna i EU är ett projekt på gång för att åstadkomma en överenskommelse för skydd av säkerhetsklassificerad information.

Det generella säkerhetsskyddsavtalet mellan Danmark, Finland, Island, Norge och Sverige undertecknades i Oslo den 7 maj 2010.

2 Nuläge

2.1 Lag om internationella förpliktelser som gäller informationssäkerhet

Lagens allmänna tillämpningsområde

Lagen om internationella förpliktelser som gäller informationssäkerhet (588/2004) stiftades i samband med att överenskommelsen om informationssäkerhet mellan Finland och Tyskland och ESA-överenskommelsen sattes i kraft. Lagen ansågs nödvändig, bland annat för att ikraftsättandet av internationella fördrag tvingar till avvikelser från våra nationella regleringar som utgår från handlingars offentlighet och säkerhet, med huvudsaklig grund i lagen om offentlighet i myndigheternas verksamhet (621/1999), nedan offentlighetslagen.

Lagen om internationella förpliktelser som gäller informationssäkerhet tillämpas på särskilt känsligt informationsmaterial. Med det avses sekretessbelagda handlingar och sekretessbelagt material och uppgifter som ingår däri som har säkerhetsklassificerats i enlighet med en internationell säkerhetsförpliktelse. Särskilt känsligt informationsmaterial är således till en finländsk myndighet lämnade handlingar och uppgifter i dem, vilka avsändaren i enlighet med en internationell överenskommelse som är bindande för Finland eller med någon annan internationell förpliktelse har försett med en anteckning om säkerhetsklassificering. Lagen kan endast tillämpas om den internationella överenskommelsen har satts i kraft i Finland på det sätt som grundlagen kräver eller om det är fråga om en internationell förpliktelse som annars är bindande för Finland.

Till kategorin särskilt känsligt informationsmaterial som omfattas av lagens tillämpningsområde hänförs dessutom handlingar som har upprättats av en finländsk myndighet, eller av en näringsidkare som hör till lagens tillämpningsområde, och av vilka det framgår information som ingår i handlingar som har sänts till Finland eller information som kan hämtas ur sådant material. Vidare omfattar lagens tillämpningsområde handlingar och material som har framställts i Finland utgående från säkerhetsklassificerad information.

Lagens säkerhetsförpliktelser ska tillämpas också då den överenskommelse eller författning som tillämpningen av bestämmelserna baserar sig på inte längre är i kraft (15 §). Tillämpningen fortsätter så länge det är nödvändigt med tanke på det allmänna intresse som ligger till grund för säkerhetsklassificeringen.

Lagens förhållande till offentlighetslagstiftningen

Lagen om internationella förpliktelser som gäller informationssäkerhet innehåller flera bestämmelser som avviker från bestämmelserna om informationssäkerhet för nationella handlingar. I lagen ingår emellertid en allmän hänvisning till offentlighetslagen. Till de delar som finländska myndigheters handlingar innehåller annan information om internationellt samarbete än sådan som omfattas av internationella förpliktelser om informationssäkerhet ska offentlighetslagen och med stöd av den utfärdade bestämmelser tillämpas. Lagen innehåller dessutom en specialbestämmelse om beslutanderätten i situationer där det med stöd av offentlighetslagen frågas efter information om särskilt känsligt material. Enligt offentlighetslagen kan en begäran om information behandlas och avgöras av den myndighet som förfogar över handlingen. En begäran om att få ta del av en handling kan emellertid överföras till en annan myndighet för beslut i sådana situationer som anges i 15 § i offentlighetslagen.

Tillämpning av lagen på näringsidkare

Lagen tillämpas förutom på myndigheter också på näringsidkare och deras anställda i sådana fall då näringsidkaren är part i ett säkerhetsklassificerat avtal eller deltar i ett upphandlingsförfarande innan ett sådant avtal sluts eller är underleverantör för en sådan näringsidkare (1 § 2 mom.).

Med ett säkerhetsklassificerat kontrakt avses ett kontrakt som en myndighet i en annan stat eller ett företag som har hemvist i den andra staten eller en internationell organisation eller ett internationellt organ, på det sätt som avses i en internationell förpliktelse som gäller informationssäkerhet, har för avsikt att ingå eller har ingått med en näringsidkare som har hemvist i Finland, om deltagande i ett anbudsförfarande eller fullgörande av ett kontrakt kan förutsätta tillgång till särskilt känsligt informationsmaterial (2 § 3 punkten).

Enligt lagen kan en näringsidkare be om en utredning över sin tillförlitlighet och om en bedömning på basis av utredningen för att kunna delta i ett anbudsförfarande som ordnas av en myndighet i en annan stat eller av ett företag som har hemvist i den andra staten, oberoende av om Finland har ingått en överenskommelse som innehåller bestämmelser om förpliktelser som gäller informationssäkerhet med den andra staten (1 § 3 mom.). Syftet med denna bestämmelse är att säkerställa finländska företags möjligheter att konkurrera om upphandlingar också när det inte finns någon internationell överenskommelse om informationssäkerhet som kan tillämpas på upphandlingen. De flesta stater förutsätter dock att det finns en bilateral överenskommelse om informationssäkerhet förrän de godkänner ett utländskt säkerhetsintyg.

En näringsidkare och den som är anställd av eller handlar på uppdrag av en näringsidkare har sekretessplikt i fråga om särskilt känsligt informationsmaterial (6 och 7 §). En näringsidkare är också skyldig att lämna nödvändig information samt att tillåta att representanter för myndigheter, internationella organ och fördragsslutande slutande stater bekantar sig med näringsidkarens säkerhetsarrangemang och lokaler, när det är nödvändigt för att uppfylla internationella förpliktelser som gäller informationssäkerhet (16 § 2 mom., 18 § 2 mom.).

Verkställande myndigheter

Lagen innehåller bestämmelser (4 §) om de myndigheter som ska sköta internationella förpliktelser som gäller informationssäkerhet. Utrikesministeriet är Finlands nationella säkerhetsmyndighet (National Security Authority, NSA) i uppfyllandet av internationella förpliktelser som gäller informationssäkerhet. Försvarsministeriet, huvudstaben, skyddspolisen och Kommunikationsverket är utsedda säkerhetsmyndigheter (Designated Security Authority, DSA). Utöver annat kan det höra till dessa myndigheter att säkerhetsklassificera handlingar i anslutning till anbuds- och upphandlingsförfaranden.

Skyddspolisen och huvudstaben svarar för utredningar som gäller personsäkerhet (11 §). Säkerhetsutredningar som gäller sammanslutningar hör enligt lagen till skyddspolisen, utom när det gäller försvarsanskaffningar, då de görs av huvudstaben (12 §). Enligt 5 § 2 mom. i lagen om internationella förpliktelser som gäller informationssäkerhet kan den nationella säkerhetsmyndigheten och de utsedda säkerhetsmyndigheterna, oavsett vad som föreskrivs om behörighet att göra säkerhetsutredningar som gäller sammanslutningar, komma överens om att sköta en viss uppgift eller uppgiftshelhet för en annan säkerhetsmyndighets räkning, om arrangemanget är nödvändigt för att få uppgifterna ändamålsenligt, ekonomiskt och smidigt skötta.

I lagen har det tidigare inte utsetts någon myndighet som skulle ha i uppgift att bedöma säkerheten i fråga om informationssystem och telekommunikation.

I 4 § 1 mom. i den av riksdagen den 1 oktober 2010 antagna lagen om ändring av lagen om internationella förpliktelser som gäller informationssäkerhet (885/2010) utsågs Kommunikationsverket till utsedd säkerhetsmyndighet.

I lagen om internationella förpliktelser som gäller informationssäkerhet finns det bestämmelser om myndigheters och näringsidkares informationsskyldighet (16 §). Syftet med bestämmelserna är att säkerställa att behöriga säkerhetsmyndigheter får den infor-

mation de behöver för att sköta sina uppgifter. Myndigheterna kan också utan hinder av bestämmelserna om sekretess lämna ut sekretessbelagd information till den utländska fördragsslutande parten för samarbete som är baserat på en internationell förpliktelse om informationssäkerhet (17 §). Vidare har en myndighet rätt att inom ramen för en internationell förpliktelse om informationssäkerhet låta representanter för internationella organisationer och organ samt för fördragsslutande stater bekanta sig med sina säkerhetsarrangemang och lokaler, oberoende av vad som föreskrivs om sekretessbeläggning av säkerhetsarrangemangen eller vad som föreskrivs eller bestäms om tillträde till utrymmen där sekretessbelagd information hanteras eller förvaras (18 §).

Den nationella säkerhetsmyndigheten ska enligt lagen i sådana fall som avses i en internationell förpliktelse om informationssäkerhet underrätta den andra fördragsslutande parten om det har kommit till dess kännedom att sekretessen hos säkerhetsklassificerad information har äventyrats eller om att det har skett överträdelser av informationssäkerhetsbestämmelserna, samt vidta åtgärder för att utreda ärendet och väcka åtal mot de skyldiga (19 §).

Sekretessbeläggning och reglering av informationsanvändningen

Lagen om internationella förpliktelser som gäller informationssäkerhet utgick tidigare från att särskilt känsligt informationsmaterial ska sekretessbeläggas (6 § 1 mom.). Sekretessplikten gäller också näringsidkare som är parter i säkerhetsklassificerade kontrakt.

I de fördrag som Finland har ingått, i praktiken bilaterala överenskommelser, som gäller utbyte av sekretessbelagd information mellan olika länders myndigheter, ingår i regel en bestämmelse som begränsar användningen av informationen. Sålunda får särskilt känsligt informationsmaterial användas och överlåtas endast för angivet ändamål, om inte den som har klassificerat materialet har samtyckt till något annat (6 § 2 mom.). Användningen av särskilt känsligt informationsmaterial är sålunda strikt ändamålsbunden.

I oktober 2010 gjordes en ändring i 6 § 1 mom. i lagen om internationella förpliktelser som gäller informationssäkerhet, så att sekretessen är beroende av innehållet i respektive avtal eller annan internationell förpliktelse (RP 53/2010 rd - RSv 135/2010 rd). En ändring av lagen var nödvändig bland annat för att det föreliggande generella säkerhetsskyddsavtalet mellan de nordiska länderna ska kunna godkännas och sättas i kraft i Finland, eftersom avtalet inte förutsätter ovillkorlig informationssekretess. Lagändringen trädde i kraft den 1 november 2010.

Säkerhetsklassificering och -åtgärder

I lagen föreskrivs om skyldigheten att förse särskilt känsligt informationsmaterial med anteckning om säkerhetsklass. Anteckningen anger vilka åtgärder som ska iakttas vid hanteringen av materialet (8 §). Ju högre materialets säkerhetsklass är, desto strängare förutsätts säkerhetsåtgärderna vara. Lagen innehåller en allmän förpliktelse att tillämpa de bestämmelser om hantering av informationsmaterialet som materialets säkerhetsklass förutsätter samt ett bemyndigande att genom förordning av statsrådet föreskriva om sådana tekniska säkerhetsåtgärder vid hantering av särskilt känsligt informationsmaterial som svarar mot materialets säkerhetsklassificering (9 §). I 11 § i statsrådets förordning om informationssäkerheten inom statsförvaltningen (681/2010), nedan kallad informationssäkerhetsförordningen, finns det föreskrifter om särskilda bestämmelser om anteckningen om säkerhetsklassificering och i 12 § om säkerhetsklassificeringens motsvarighet.

Vid hantering av säkerhetsklassificerat material ska det enligt lagen ses till att materialet förvaras i ändamålsenliga utrymmen. Om kraven på säkerheten i sådana utrymmen föreskrivs i 14 § i informationssäkerhetsförordningen.

I lagen om internationella förpliktelser som gäller informationssäkerhet har det krav skrivits in som är vanligt i internationella överenskommelser om att myndigheterna ska iaktta stor restriktivitet vid hanteringen av säkerhetsklassificerad information och att endast personer som behöver informationen för skötseln av sina uppgifter ska ges tillgång till den. Dessa personer ska namnges på förhand om detta förutsätts i överenskommel-

sen. Detsamma gäller näringsidkare som avses i 1 § 2 mom. (6 § 3 mom.).

Personsäkerhet

Sådan personsäkerhetsutredning som en internationell förpliktelse om informationssäkerhet förutsätter ska göras på det sätt som föreskrivs i och med stöd av lagen om säkerhetsutredningar (177/2002). Följaktligen fastställs t.ex. dens rättigheter som är föremål för utredningen enligt denna lag.

I lagen om internationella förpliktelser som gäller informationssäkerhet ingår emellertid två bestämmelser som är specialbestämmelser i förhållande till lagen om säkerhetsutredningar. En begränsad säkerhetsutredning kan göras också i andra fall än de som räknas upp i 19 § i lagen om säkerhetsutredningar, om en sådan är nödvändig för att fullgöra en internationell förpliktelse om informationssäkerhet (11 § 1 mom.). En annan specialbestämmelse reglerar myndigheternas befogenheter. Säkerhetsutredningen ska göras av huvudstaben då en sådan behövs för att fullgöra en internationell förpliktelse som gäller försvarsförvaltningen eller anskaffningar av försvarsmateriel. Andra säkerhetsutredningar som avser personer ska handläggas av skyddspolisen (11 § 2 mom.). Enligt 10 § 2 mom. i lagen om säkerhetsutredningar får den behöriga myndighetens bedömning av tillförlitligheten eller lämpligheten för en tjänst eller ett uppdrag hos den som utredningen gäller inte ingå i en säkerhetsutredning, om inte ett fördrag eller någon annan internationell förpliktelse som avses i lagens 9 § förutsätter det. Eftersom huvudregeln är att en säkerhetsutredning inte innehåller någon bedömning av en persons tillförlitlighet nämns bedömningen av en persons tillförlitlighet särskilt i lagen om internationella förpliktelser som gäller informationssäkerhet. En sådan bedömning ska på basis av säkerhetsutredningen göras av den nationella säkerhetsmyndigheten eller, om så har överenskommits mellan säkerhetsmyndigheterna, av den för uppgiften utsedda säkerhetsmyndigheten (1 § 3 mom.).

Utgående från bedömningen utfärdas det ett personligt säkerhetsintyg (Personal Security Clearance Certificate). Intyget skickas vanligtvis till den fördragsslutande partens säkerhetsmyndighet på det sätt som anges i fördraget. I lagen föreskrivs det också om överlämnande av intyget till vederbörande själv (14 §).

Säkerhetsutredning som gäller sammanslutning

Säkerhetsutredningar som gäller sammanslutningar ska dels säkerställa att lokaler och hanteringspraxis är ändamålsenliga, dels personalens kompetens. Bedömningen av en näringsidkares tillförlitlighet avser framför allt hur väl näringsidkaren kan skydda säkerhetsklassificerad information. Säkerhetsförfarandet när det gäller en sammanslutning och den därpå baserade bedömningen utgår huvudsakligen från information som näringsidkaren själv lämnar samt från en säkerhetskartläggning av näringsidkarens lokaler, och nödvändiga åtgärder vidtas med hjälp av ett avtal som ingås med näringsidkaren. Huvudstaben svarar för dessa utredningar i frågor som hör till försvarsförvaltningen, skyddspolisen i andra frågor. Vid utredningen ska de omständigheter som anges i lagen om internationella förpliktelser som gäller informationssäkerhet beaktas, däribland hur man kan skydda säkerhetsklassificerad information från att obehörigen röjas, ändras eller förstöras eller hur man kan förhindra obehörigt tillträde till utrymmen där säkerhetsklassificerad information hanteras eller där det bedrivs verksamhet som avses i ett säkerhetsklassificerat kontrakt (12 §).

Huvudstaben kan med näringsidkare som hör till lagens tillämpningsområde ingå avtal om att näringsidkaren förbinder sig att vidta åtgärder för att uppfylla internationella förpliktelser om informationssäkerhet (13 §). I avtalet kan de åtgärder närmare preciseras som näringsidkaren ska vidta för att uppfylla de krav som följer av internationella förpliktelser som gäller informationssäkerhet. I avtalet förbinder sig näringsidkaren också att justera sin verksamhet i enlighet med säkerhetskartläggningen. Efter säkerhetsutredning och eventuellt avtal kan huvudstaben göra en bedömning av näringsidkarens tillförlitlighet och utfärda ett säkerhetsintyg (Facility Security Clearance Certificate). På grund av förslaget till ändring av 13 § i lagen om internationella förpliktelser som gäller informa-

tionssäkerhet kommer motsvarande förfarande för förbindelser att genomföras också i de säkerhetsutredningar angående sammanslutningar som skyddspolisen utför.

2.2 Lagstiftning om säkerhetsutredningar

Bestämmelser om säkerhetsutredningar som hänför sig till personalsäkerhet finns i lagen om säkerhetsutredningar. Syftet med lagen är att genom utredningsförfarandet öka möjligheterna att förebygga brott som kan medföra allvarlig skada för viktiga allmänna eller enskilda intressen eller för datasäkerhet av synnerligen stor betydelse.

En säkerhetsutredning kan göras över en person som söker en tjänst eller ett uppdrag, som ska anställas eller antas till utbildning eller som sköter en tjänst eller ett uppdrag och den kan vara normal, omfattande eller begränsad. Säkerhetsutredningar görs i de fall som anges i lagen, t.ex. om ett fördrag eller någon annan internationell förpliktelse som är bindande för Finland förutsätter att en säkerhetsutredning görs eller att ett intyg över en sådan visas upp.

Eftersom integritetsskyddet har karaktären av grundläggande rättighet är utredningsförfarandet strikt formbundet. En säkerhetsutredning kan göras endast om den som utredningen gäller i förväg har gett sitt uttryckliga, skriftliga samtycke. I lagen ingår också en uttömmande uppräkning över de register som får användas vid utredningsförfarandet.

Var och en har rätt att få veta om det har gjorts en säkerhetsutredning över en själv för något bestämt uppdrag. Den som utredningen gäller har också rätt att av den behöriga myndigheten på begäran få de uppgifter som en normal eller omfattande utredning innehåller om vederbörande. Denna rätt gäller emellertid inte information som hämtats ur ett register som en registrerad inte har rätt till insyn i.

Justitieministeriet har tillsatt en arbetsgrupp för den aktuella översynen av lagen om säkerhetsutredningar. Den har i uppdrag att utveckla lagen om säkerhetsutredningar så att den stämmer överens med skyldigheter som är bindande för Finland och med allmän internationell praxis. Målet är att arbetsgruppens arbete ska utmynna i en regeringsproposition år 2011.

3 Målsättning

Syftet med propositionen är att sätta i kraft det generella säkerhetsskyddsavtalet om ömsesidigt skydd och utbyte av säkerhetsskyddsklassificerade uppgifter mellan Danmark, Finland, Island, Norge och Sverige och därigenom förbättra samarbetet mellan de nordiska länderna samt att trygga finländska företags möjligheter att delta i internationella och nordiska projekt som kan kräva utbyte av känslig information.

4 Propositionens konsekvenser

4.1 Konsekvenser för medborgarna

Genom att avtalet sätts i kraft kommer lagen om internationella förpliktelser som gäller informationssäkerhet att tillämpas på säkerhetsklassificerad information och säkerhetsklassificerat material som sänds från de andra nordiska länderna till Finland. I lagen ingår en specialbestämmelse om att handlingar, och informationen de innehåller, som hos den andra fördragsslutande parten är sekretessbelagda eller säkerhetsklassificerade ska vara sekretessbelagda också i Finland. Till sin utformning skiljer sig bestämmelsen från vad som föreskrivs i offentlighetslagen om sekretessbeläggning i allmänt intresse, eftersom sekretessen där i de flesta fall är beroende av konsekvenserna för det skyddade intresset ifall uppgifterna lämnades ut. Sekretessbestämmelserna i lagen om internationella förpliktelser som gäller informationssäkerhet har sålunda en mera heltäckande ordalydelse än den allmänna offentlighetslagen. Genom lagen som trädde i kraft den 1 november 2010 ändrades emellertid 6 § så att känsligt informationsmaterial framöver ska sekretessbeläggas, om inte något annat följer av en internationell förpliktelse som gäller informationssäkerhet. Avtalet mellan Finland och de nordiska länderna gäller handlingar som en fördragsslutande part anser att ska vara sekretessbelagd och följaktligen har försett med hög säkerhetsklassificering. Denna typ av handlingar är i regel sekretessbelagda också enligt 24 § 1 mom. 2 punkten i offent-

lighetslagen. Den största skillnaden består i att den myndighet som ska besluta om upprättandet av en handling som avses i den internationella förpliktelsen om informationssäkerhet inte särskilt behöver motivera den skada som orsakas om informationen röjs. I övrigt ska en begäran om information behandlas i enlighet med offentlighetslagen. Om det uppkommer oklarheter om huruvida klassificeringen är korrekt eller om vilken information i handlingen det är som föranleder klassificeringen, ska myndigheten kontakta den fördragsslutande part som har upprättat handlingen.

Med stöd av det som anförts ovan kan bedömningen göras att förslaget om att sätta i kraft avtalet om säkerhetsskydd mellan de nordiska länderna strängt taget inte minskar medborgarnas tillgång till information i jämförelse med tillgången till information i enlighet med den allmänna lagstiftningen.

Personalsäkerheten är en viktig del av informationssäkerheten. Eftersom lagen om internationella förpliktelser som gäller informationssäkerhet i sig förutsätter att det förfarande som avses i lagen om säkerhetsutredningar används för att kontrollera anställdas tillförlitlighet, innebär ett godkännande av den föreslagna lagen inte inskränkningar jämfört med tidigare i skyddet av medborgarnas personliga integritet och personuppgifter.

4.2 Konsekvenser för näringslivet

Avtalet öppnar en möjlighet för den finländska industrin att få beställningar eller att delta i projekt som förutsätter tillgång till information som är säkerhetsklassificerad i de nordiska länderna. Analogt öppnar avtalet en möjlighet för industrin i de andra nordiska länderna att få beställningar eller att delta i projekt som förutsätter tillgång till information som är säkerhetsklassificerad i Finland.

4.3 Ekonomiska konsekvenser

Propositionen medför inga konsekvenser för statsfinanserna eller andra mera än obetydliga ekonomiska konsekvenser.

4.4 Konsekvenser för förvaltningen

Godkännandet av det avtal och den lag som ingår i propositionen medför inga skyldigheter till eller behov av förändringar i förvaltningen.

5 Beredningen av propositionen

Statsrådets allmänna sammanträde beslöt den 26 maj 2005 att tillsätta en förhandlingsdelegation. Till Finlands delegation hörde som medlemmar företrädare för justitieministeriet, handels- och industriministeriet, försvarsministeriet och utrikesministeriet.

Efter att förhandlingsdelegationen hade tillsatts inleddes avtalsförhandlingarna sommaren 2005 under norsk ledning och kunde rätt långt färdigförhandlas under 2005. Slutförandet fördröjdes dock av Danmarks ovilja att gå vidare, eftersom de danska myndigheterna inte såg något större behov av avtalet. Finland och Sverige drev hårt på vidare förhandlingar eftersom avtalet har betydelse särskilt för dessa länders försvarsförvaltning.

Hösten 2008 fortsatte förhandlingarna i Oslo. Under tiden förnyades avtalet och förenklades för att motsvara de senaste kraven på informationssäkerhet. Finland spelade en aktiv roll i förhandlingarna tack vare sitt modellavtal. Avtalet färdigställdes och det fick sedan vänta på Danmarks samtycke till undertecknande. I början av pågående år meddelade Danmark att landet är redo att underteckna avtalet, och den 7 maj 2010 undertecknades det i Oslo. Propositionen har beretts som tjänsteuppdrag vid utrikesministeriet. I beredningen av avtalet och i förhandlingarna har representanter för utrikesministeriet, justitieministeriet, försvarsministeriet samt arbets- och näringsministeriet deltagit.

Utlåtanden om propositionen har begärts av justitieministeriet, arbets- och näringsministeriet, försvarsministeriet, finansministeriet, inrikesministeriet, kommunikationsministeriet, skyddspolisen, huvudstaben, Kommunikationsverket samt Finlands Näringsliv EK.

Utlåtandena har beaktats i den slutliga bearbetningen av propositionen.

DETALJMOTIVERING

1 Avtalets innehåll och förhållande till lagstiftningen i Finland

Artikel 1. Syfte och tillämpningsområde. I stycke 1 anges det att syftet med avtalet är att skydda säkerhetsklassificerade uppgifter som utbyts mellan två nordiska länder eller mellan kontraktsparter inom parternas respektive jurisdiktion. I artikeln anges också de funktioner avtalet tillämpas på. De är utrikes-, försvars-, säkerhets- och polisärenden samt vetenskapligt, industriellt och teknologiskt samarbete. Upprätthållandet av gränssäkerheten anses ingå i dessa områden. Avtalet tillämpas också på förmedling av uppgifter som tagits fram grundade på, eller som härrör från, de uppgifter som har utbytts.

Artikel 2. Definitioner. I artikeln definieras de begrepp som är centrala i tillämpningen av avtalet.

Med säkerhetsskyddsklassificerade uppgifter avses information, oavsett form, som enligt parternas lagstiftning kräver skydd mot förlust, obehörig åtkomst eller annat röjande och har märkts som sådan. Definitionen omfattar också information, handlingar eller annat material som tas fram utifrån de säkerhetsskyddsklassificerade uppgifterna. Detta är i samklang med 2 § 2 mom. i lagen om internationella förpliktelser som gäller informationssäkerhet.

Med upprättande part avses en part, liksom statliga organ eller offentliga och privata organisationer inom dess jurisdiktion, som delger säkerhetsskyddsklassificerad information.

Med mottagande part avses en part, liksom statliga organ eller offentliga och privata organisationer under dess jurisdiktion, till vilken säkerhetsskyddsklassificerad information är delgiven av en upprättande part.

Med säkerhetsskyddsklassificerat kontrakt avses ett kontrakt som innehåller eller avser säkerhetsskyddsklassificerade uppgifter. Detta är i samklang med 2 § 3 punkten i lagen om internationella förpliktelser som gäller informationssäkerhet.

Med behörig säkerhetsmyndighet avses en statlig myndighet som ansvarar för säkerhetsfrågor. Enligt lagen om internationella förpliktelser som gäller informationssäkerhet är denna myndighet i Finland utrikesministeriet, där Nationella säkerhetsmyndigheten har ansvaret för uppgiften. Härutöver är försvarsministeriet, skyddspolisen, huvudstaben och Kommunikationsverket särskilt utsedda säkerhetsmyndigheter.

Med kontraktstagare avses en fysisk eller juridisk person med rättslig förmåga att ingå kontrakt.

Med säkerhetsöverträdelse avses en gärning eller försummelse som bryter mot nationella säkerhetsregler och som kan medföra att säkerhetsskyddsklassificerade uppgifter äventyras eller röjs.

Med säkerhetsklarering avses ett positivt utfall av prövning av en persons eller ett företags lämplighet att ges tillgång till och hantera säkerhetsskyddsklassificerade uppgifter på viss nivå i enlighet med respektive lands säkerhetsbestämmelser. I Finland är det skyddspolisen och huvudstaben som med stöd av lagen om säkerhetsutredningar gör utredningar om personers bakgrund.

Med behörighet till säkerhetsskyddsklassificerade uppgifter (need to know) avses en princip enligt vilken tillgång till säkerhetsskyddsklassificerade uppgifter endast får ges till personer i samband med officiella uppdrag och uppgifter. Motsvarande definition ingår också i 6 § 3 mom. i lagen om internationella förpliktelser som gäller informationssäkerhet.

Med tredje part avses en institution, internationell eller nationell organisation, juridisk person eller stat som inte är part i detta avtal. En part i detta avtal betraktas som "tredje part" i samband med samarbete i vilket parten inte deltar.

Artikel 3. Skydd av säkerhetsskyddsklassificerade uppgifter. I stycke 1 åläggs parterna att vidta lämpliga åtgärder, i enlighet med den egna nationella lagstiftningen, för att skydda de säkerhetsskyddsklassificerade uppgifter som avtalet omfattar. Parterna ska se till att de säkerhetsskyddsklassificerade uppgifter som avtalet omfattar får samma nivå av säkerhetsskydd som ges för egna säkerhetsskyddsklassificerade uppgifter i motsvarande informationssäkerhetsklass, enligt definitionen i artikel 5. I 8 § i lagen om in-

ternationella förpliktelser som gäller informationssäkerhet åläggs myndigheterna att förse särskilt känsligt informationsmaterial med anteckning om säkerhetsklass. I 11 § i informationssäkerhetsförordningen finns det närmare föreskrifter om anteckningen om säkerhetsklassificering och i 12 § om deras motsvarigheter vid tillgodoseende av internationella förpliktelser som gäller informationssäkerheten.

Tillgång till säkerhetsskyddsklassificerade uppgifter på nivån CONFIDENTIAL eller högre, och tillträde till platser och anläggningar där säkerhetsskyddsklassificerade uppgifter förvaras eller där verksamhet bedrivs i vilken säkerhetsskyddsklassificerade uppgifter förekommer, ska enligt stycke 2 begränsas till dem som har säkerhetsklarerats och som har behörighet till säkerhetsskyddsklassificerade uppgifter. Bestämmelsen motsvarar bestämmelserna i 6 § 3 mom. i lagen om internationella förpliktelser som gäller informationssäkerhet och i 13 § i informationssäkerhetsförordningen och avseende anläggningars säkerhet i 10 § i lagen och i 14 § i förordningen.

Enligt stycke 3 ska parterna ömsesidigt erkänna varandras säkerhetsklareringar. Föreskrifter om personsäkerhetsutredningar finns i lagen om säkerhetsutredningar och om säkerhetsutredningar som gäller sammanslutningar i 12 § i lagen om internationella förpliktelser som gäller informationssäkerhet.

Enligt stycke 4 ska varje part se till att säkerhetslagstiftning, säkerhetsföreskrifter och säkerhetspraxis följs vid de myndigheter, företag och anläggningar, inom den egna jurisdiktionen, som förfogar över, utvecklar, framställer och/eller använder de andra parternas säkerhetsskyddsklassificerade uppgifter.

Artikel 4. Delgivning och användning av säkerhetsskyddsklassificerad information. Stycke 1 ålägger parterna att respektera principen om den upprättande partens medgivande i enlighet med deras konstitutionella bestämmelser samt nationella lagar och bestämmelser. Säkerhetsskyddsklassificerade uppgifter, som omfattas av avtalet, får inte delges tredje part eller medborgare i andra länder utan föregående skriftligt samråd med den upprättande parten. Säkerhetsskyddsklassificerade uppgifter som mottagits av någon av parterna från en annan part får endast användas för det syfte som angetts.

Alla stater garanterar inte ovillkorlig sekretess med stöd avtal, utan frågan måste avgöras från fall till fall utgående från en sådan prövning av skaderekvisitet som baserar sig på den nationella lagstiftningen. Till exempel är huvudregeln enligt den nationella lagstiftningen i Sverige (tryckfrihetsförordning SFS 1949:105) att allmänna handlingar – också från andra stater – är offentliga och att avvikelser från denna regel endast får göras om det är påkallat med hänsyn tillrikets säkerhet eller dess förhållande till annan stat eller mellanfolklig organisation. I praktiken har Sverige emellertid aldrig agerat i strid med en främmande stats sekretessbegäran. Lämnas sådana uppgifter ut utan tillstånd, kan det anses skada Sveriges relationer till den berörda staten, varvid skaderekvisitet uppfylls.

Av ovan beskriven anledning ansågs det att en förutsättning för att det nordiska informationssäkerhetsavtalet ska kunna godkännas och sättas i kraft i Finland är att 6 § 1 mom. i lagen om internationella förpliktelser som gäller informationssäkerhet ändras (RP 53/2010 vp). I propositionen motiveras ändringen av 6 § med att det vid de avtalsförhandlingar som Finland fört har framkommit sådana situationer där en avtalspart inte garanterar ovillkorlig sekretess med stöd av avtalet, utan där frågan måste avgöras från fall till fall utgående från en sådan prövning av skaderekvisitet som baserar sig på den nationella lagstiftningen. Det är inte ändamålsenligt att Finland iakttar en mera omfattande sekretess än andra avtalsparter. Av denna anledning föreslogs det i propositionen att en bestämmelse tas in i 6 § 1 mom. i lagen om internationella förpliktelser som gäller informationssäkerhet, enligt vilken sekretessen är beroende av innehållet i respektive avtal eller annan internationell förpliktelse. Lagförslaget godkändes av riksdagen utan ändringar och lagen trädde i kraft den 1 november 2010.

I 6 § 2 mom. i lagen om internationella förpliktelser som gäller informationssäkerhet föreskrivs om att särskilt känsligt informationsmaterial får användas och lämnas ut endast för angivet ändamål, om inte den som bestämt materialets säkerhetsklass har sam-

tyckt till något annat. Artikel 4 stycke 1 är i samklang med detta moment.

Enligt stycke 2 är det, i det fall att en part eller tillhörande myndigheter eller organisationer inom de områden som anges i artikel 1 tilldelar kontrakt för verksamhet i annan parts land, och om kontraktet omfattar säkerhetsskyddsklassificerade uppgifter, parten i det land i vilket den avtalade verksamheten äger rum, som ansvarar för hantering av sådana säkerhetsskyddsklassificerade uppgifter i enlighet med dess egna regler och krav.

I stycke 3 fastställs de åtgärder varje part ska vidta innan delgivning av säkerhetsskyddsklassificerade uppgifter som har mottagits av en annan part eller kontraktstagare eller möjliga kontraktstagare inom partens jurisdiktion. Parten ska a) säkerställa att sådana kontraktstagare eller möjliga kontraktstagare och deras anläggningar har möjlighet att ge de säkerhetsskyddsklassificerade uppgifterna adekvat skydd, b) se till att lämplig säkerhetsklarering finns för berörda kontraktstagares anläggningar och för all den personal som i sin tjänst behöver säkerhetsskyddsklassificerade uppgifter, c) säkerställa att personer som har tillgång till säkerhetsskyddsklassificerade uppgifter har upplysts om deras skyldighet att skydda de säkerhetsskyddsklassificerade uppgifterna i enlighet med tillämplig lagstiftning och d) utföra regelbundna säkerhetsskyddskontroller vid berörda klarerade anläggningar.

Artikel 5. Säkerhetsklasserna. I artikeln fastställs att säkerhetsskyddsklassificerade uppgifter ska förses med någon av följande fyra beteckningar för informationssäkerhetsklasser:

Den högsta säkerhetsklassen, som kräver de strängaste informationssäkerhetsåtgärderna, är ”ERITTÄIN SALAINEN/YTTERST HEMLIG” (TOP SECRET). Till kategorin ytterst hemlig räknas i Finland information som, om den obehörigen röjs, kan orsaka särskilt påtaglig skada för försvaret, säkerheten, de internationella relationerna eller andra allmänna intressen. Finlands internationella relationer skyddas i 24 § 1 mom. 1 och 2 punkten i offentlighetslagen, försvaret i 10 punkten och säkerheten i 5, 8 och 9 punkten i samma moment. Andra allmänna intressen som avses i definitionen kan till exempel vara skyddet av säkerhetsarrangemangen för statsledningen och statsbesök samt för datasystem (24 § 1 mom. 7 punkten) samt samhällsekonomin (24 § 1 mom. 11 och 12 punkten).

Den nästhögsta säkerhetsklassen är ”SALAINEN/HEMLIG” (SECRET). Till denna kategori hör i Finland information som, om den obehörigen röjs, kan orsaka väsentlig skada för försvaret, säkerheten, de internationella relationerna eller andra allmänna intressen.

Den tredje högsta säkerhetsklassen är ”LUOTTAMUKSELLINEN/KONFIDENTIELL” (CONFIDENTIAL) varmed i Finland avses information som, om den obehörigen röjs, kan skada försvaret, säkerheten, de internationella relationerna eller andra allmänna intressen.

Till den fjärde säkerhetsklassen ”KÄYTTÖ RAJOITETTU/BEGRÄNSAD TILLGÅNG” (RESTRICTED) hör information som, om den obehörigen röjs, kan skada allmänna intressen eller försämra myndigheternas möjligheter att agera.

Särskilda bestämmelser om anteckningen om säkerhetsklassificering finns i 11 § och om säkerhetsklassificeringarnas motsvarigheter i 12 § i informationssäkerhetsförordningen. En särskild bestämmelse om anteckningen om säkerhetsklassificering på svenska finns i 11 § 4 mom. i förordningen.

Enligt stycke 2 får den mottagande parten inte ändra informationssäkerhetsklass på de säkerhetsskyddsklassificerade uppgifter som mottagits, utan att detta har föregåtts av upprättande parts skriftliga medgivande. Den upprättande parten ska informera den mottagande parten om ändringar som görs i informationssäkerhetsklassning av den information som har utbytts.

Enligt stycke 3 ska den mottagande parten förse säkerhetsskyddsklassificerade uppgifter som har mottagits med den egna beteckningen för motsvarande informationssäkerhetsklass. Översättningar och kopior ska förses med beteckning för samma informationssäkerhetsklass som originalet.

Enligt stycke 4 ska uppgifter från Sverige som endast har beteckningen ”HEMLIG” betraktas som HEMLIG/SECRET. Bestämmelser om anteckningen på kopior av klassificerade handlingar finns i 17 § 2 mom. i informationssäkerhetsförordningen.

Artikel 6. Behöriga säkerhetsmyndigheter och säkerhetssamarbete. I stycke 1 föreskrivs att de behöriga säkerhetsmyndigheterna ska övervaka genomförandet av avtalet. Enligt stycke 2 ska parterna meddela varandra om vilka säkerhetsmyndigheter som är behöriga och om ändringar görs i detta avseende.

I stycke 3 konstateras att de behöriga säkerhetsmyndigheterna på begäran ska förse varandra med information om deras nationella lagar och bestämmelser, standarder, metoder och praxis för skydd av säkerhetsskyddsklassificerade uppgifter för att åstadkomma och upprätthålla jämförbara säkerhetsstandarder. För att uppnå detta mål får de behöriga säkerhetsmyndigheterna besöka varandra.

I stycke 4 konstateras det att de behöriga säkerhetsmyndigheterna ska informera varandra om alla relevanta säkerhetshot som kan äventyra delgivna säkerhetsskyddsklassificerade uppgifter.

I stycke 5 och 6 fastställs de behöriga myndigheternas skyldighet att på begäran bistå varandra med att i enlighet med nationell lagstiftning genomföra säkerhetsklareringsärenden och att skyndsamt informera varandra om förändringar i ömsesidigt erkända säkerhetsklareringar.

Enligt stycke 7 får parternas underrättelse- och säkerhetstjänster, i enlighet med nationell lagstiftning, utbyta operativ eller underrättelseinformation direkt mellan sig.

Artikel 7. Besök. Artikeln innehåller bestämmelser om de förfaranden som ska följas när de fördragsslutande parterna sinsemellan ordnar besök som medför tillgång till säkerhetsskyddsklassificerade uppgifter eller till områden där verksamheten anknyter till sådana uppgifter eller där sådana uppgifter lagras eller hanteras. Enligt stycke 1 kräver besök skriftligt förhandstillstånd av värdlandets behöriga säkerhetsmyndighet, om de medför tillgång till säkerhetsskyddsklassificerade uppgifter på nivån CONFIDENTIAL eller högre, eller till områden där sådana säkerhetsskyddsklassificerade uppgifter tas eller kan tas fram, hanteras eller lagras.

Enligt stycke 2 kan besök tillåtas förutsatt att besökarna har säkerhetsklarerats av den behöriga myndigheten hos den sändande parten och de är behöriga att ta del av säkerhetsskyddsklassificerade uppgifter i enlighet med värdlandets nationella lagar och bestämmelser (t.ex. informationsbehov). En ytterligare förutsättning för att ett besök ska tillåtas är att besökarna av värdlandets behöriga säkerhetsmyndighet har getts behörighet att genomföra nödvändiga besök. Den sistnämnda förutsättningen berör endast avtalsparter, vilkas nationella system förutsätter att behörighet medges.

En besöksförfrågan (Request for visit, RfV) ska enligt stycke 3 lämnas till värdlandets behöriga säkerhetsmyndighet senast 10 dagar före besöket. I brådskande fall kan de behöriga myndigheterna avtala om en kortare tid. Närmare bestämmelser om vilken information som ska ingå i förfrågan finns i stycke 4 och i stycke 5 konstateras det att förfrågan ska göras i enlighet med de principer som har överenskommits av de behöriga säkerhetsmyndigheterna.

Enligt stycke 6 gäller tillstånd för upprepade besök i högst 12 månader. Enligt stycke 7 får värdparten, om det är nödvändigt, kräva ett certifikat över säkerhetsklarering. Andra besöksrutiner får enligt stycke 8 tillämpas om parternas behöriga säkerhetsmyndigheter har kommit överens om det.

Artikel 8. Säkerhetsskyddsklassificerade kontrakt. Artikeln innehåller bestämmelser om situationer där en fördragsslutande part ingår, eller ger en kontraktspart inom sin jurisdiktion tillstånd att ingå, ett säkerhetsskyddsklassificerat kontrakt med en kontraktspart som lyder under en annan fördragsslutande parts jurisdiktion.

Enligt stycke 1 får den behöriga säkerhetsmyndigheten för den part som vill sluta ett säkerhetsskyddsklassificerat kontrakt med kontraktstagare i en annan parts land på förhand begära en säkerhetsklarering som utfärdats för den aktuella kontraktstagarens anläggningar av den andra partens behöriga säkerhetsmyndighet. Om kontraktstagaren saknar en säkerhetsklarering, får den part som vill sluta ett säkerhetsskyddsklassificerat kontrakt begära av den part som kontraktstagaren tillhör att en säkerhetsklarering utfärdas i enlighet med nationella lagar och bestämmelser. Enligt stycke 2 får vid öppen anbudsgivning, som inte är riktad till något särskilt land eller företag, den mottagande partens säkerhetsmyndighet likväl utan formell begäran lämna relevanta säkerhetscertifikat till den upprättande partens säkerhets-

myndighet. Syftet med bestämmelsen är att försnabba finländska eller analogt andra nordiska företags tillträde till säkerhetsklassificerad information som krävs för en offert, vilket i sin tur gör företagens offertberedning effektivare och konkurrensställning bättre.

Enligt stycke 3 ska säkerhetsskyddsklassificerade kontrakt innehålla tillämpliga säkerhetsbestämmelser och kompletteras med dokumentation som identifierar den information eller de beståndsdelar eller förhållanden som är säkerhetsskyddsklassificerade i kontraktet. I stycke 4 föreskrivs det att det är den behöriga säkerhetsmyndigheten för den part som tecknar kontraktet som ska säkerställa att kopior av all tillämplig säkerhetsrelaterad dokumentation som berör det säkerhetsskyddsklassificerade kontraktet kommer den behöriga säkerhetsmyndigheten i det land där kontraktet ska utföras tillhanda.

Nationella bestämmelser om säkerhetsklassificerade kontrakt finns i 1 § 2 mom. (tillämpning på näringsidkare), i 2 § 2 punkten (särskilt känsligt informationsmaterial) och i 3 kap. om åtgärder som gäller informationssäkerhet i lagen om internationella förpliktelser som gäller informationssäkerhet. Bestämmelserna i avtalet motsvarar till denna del den nationella regleringen. Föreskrifter om finska myndigheters rätt att lämna ut information som behövs för att uppfylla förpliktelsen finns i 17 § i lagen om internationella förpliktelser som gäller informationssäkerhet.

Artikel 9. Översättning, reproduktion och förstöring av säkerhetsskyddsklassificerade uppgifter.

Artikeln innehåller bestämmelser om översättning, kopiering och förstöring av material i olika säkerhetsklasser.

Enligt stycke 1 ska alla reproduktioner och översättningar vara försedda med tillämplig märkning av säkerhetsskyddsklassificering och skyddas som den säkerhetsskyddsklassificerade originalinformationen. Antalet översättningar och reproduktioner ska begränsas till ett minimum som är nödvändigt för ett officiellt syfte. I stycke 2 bestäms att alla översättningar ska innehålla en anteckning på det översatta språket som visar att de innehåller säkerhetsskyddsklassificerade uppgifter från den upprättande parten. Motsvarande bestämmelser finns i 17 § i informationssäkerhetsförordningen.

I stycke 3 förutsätts det att säkerhetsskyddsklassificerad information som markerats TOP SECRET endast får översättas eller reproduceras efter ett skriftligt tillstånd från den upprättande parten. Enligt stycke 4 får information som markerats TOP SECRET inte förstöras utan ska återlämnas till den upprättande parten när den inte längre bedöms nödvändig av avtalsparterna. Syftet med föreskriften är att säkerställa att informationen sparas, till exempel i fall då materialet eller en del av det enligt arkivlagstiftningen ska bevaras. Information i säkerhetsklassen SECRET eller lägre får enligt stycke 5 förstöras i enlighet med nationella lagar och bestämmelser efter det att den inte längre bedöms nödvändig. Bestämmelser om arkivering av klassificerade handlingar finns i arkivlagen (831/1994). Bestämmelser om förstöring av dem finns i 21 § i informationssäkerhetsförordningen.

I stycke 6 förskrivs om situationer där en krissituation omöjliggör skyddet av säkerhetsskyddsklassificerade uppgifter. I sådana fall ska de omedelbart förstöras och den mottagande parten så snart som möjligt meddela den behöriga säkerhetsmyndigheten i den upprättande parten om förstöringen av de säkerhetsskyddsklassificerade uppgifterna.

Artikel 10. Överföring av säkerhetsskyddsklassificerade uppgifter. Artikeln innehåller bestämmelser om tillvägagångssättet vid överföring av säkerhetsklassificerad information mellan de fördragsslutande parterna. Enligt stycke 1 ska uppgifterna förmedlas via med diplomatpost eller kurirer, om inte de relevanta behöriga säkerhetsmyndigheterna kommit överens om annat. I stycke 2 föreskrivs att om någon av parterna önskar överföra säkerhetsskyddsklassificerad information utanför sitt territorium ska en sådan överföring koordineras med den upprättande parten innan överföringen. Bestämmelsen är i samklang med 18 § om förmedling av en handling i informationssäkerhetsförordningen.

Artikel 11. Säkerhetsöverträdelser. När en säkerhetsöverträdelse som inbegriper förlust eller röjande av säkerhetsskyddsklassificerade uppgifter som omfattas av avtalet, ska enligt stycke 1 den behöriga säkerhetsmyndig-

heten i det land där säkerhetsöverträdelsen sker informera berörda parters säkerhetsmyndigheter så snart som möjligt. Enligt stycke 2 ska den part som har jurisdiktion vidta relevanta åtgärder som är tillåtna enligt nationell lagstiftning för att begränsa de konsekvenser som säkerhetsöverträdelsen har medfört och förebygga ytterligare säkerhetsöverträdelser eller skador. Enligt stycke 3 ska övriga berörda parter på begäran bistå utredningen. De fördragsslutande parterna ska informeras om utredningens resultat och de åtgärder som har vidtagits till följd av säkerhetsöverträdelsen. Vidare ska parterna i ett slutligt yttrande underrättas om skälen till och omfattningen av säkerhetsöverträdelsen, samt erhålla information om vilka åtgärder som vidtagits för att undvika upprepning. Bestämmelserna som krävs för att genomföra de förpliktelser som avses i artikeln ingår i 19 § i lagen om internationella förpliktelser som gäller informationssäkerhet.

Artikel 12. Kostnader. Parterna ersätter inte varandra för eventuella kostnader som uppstår för dem inom ramen för avtalet.

Artikel 13. Tvistlösning. Tvister mellan parterna om tolkningen eller tillämpningen av avtalet ska lösas genom samråd och inte hänskjutas till nationell eller internationell domstol eller tredje part för avgörande.

Artikel 14. Slutbestämmelser. Artikeln innehåller bestämmelser om godkännande, godtagande eller ratifikation, ikraftträdande, ändring och uppsägning av avtalet. Enligt stycke 1 är Konungariket Norges regering depositarie för ratifikations-, godtagande- eller godkännandeinstrumenten. Enligt stycke 2 träder avtalet i kraft trettio dagar efter det datum då ratifikations-, godtagande- eller godkännandeinstrumenten lämnats in av den sista av de regeringar som undertecknat avtalet. Enligt stycke 3 får dock varje part fram till att avtalet träder i kraft då den lämnar sitt ratifikations-, godtagande- eller godkännandeinstrument eller vid en senare tidpunkt meddela att den anser sig vara bunden av avtalet i förhållande till någon annan part som har lämnat liknande meddelande. Dessa meddelanden träder ikraft trettio dagar efter dagen för mottagandet av meddelandet. Syftet med bestämmelsen är att avtalet innan det träder i kraft, om de fördragsslutande parterna så önskar, ska kunna tillämpas temporärt mellan de stater som får sina nationella godkännandeprocedurer slutförda i snabbare takt. Avsikten är att Finland ska lämna ett sådant meddelande.

Enligt stycke 4 får ändringar i avtalet när som helst göras skriftligen på gemensam överenskommelse mellan parterna. Enligt stycke 5 träder godkända ändringar i kraft den trettionde dagen efter det att samtliga parter har meddelat depositarien sitt godkännande. Enligt stycke 6 är avtalet, när det har trätt i kraft, öppet för anslutning av tredje stat efter undertecknande regeringars godkännande. Anslutningsinstrumenten ska lämnas till Konungariket Norges regering. För varje anslutande stat träder avtalet enligt stycke 7 i kraft på den trettionde dagen efter det att staten lämnat sitt anslutningsinstrument.

Enligt stycke 8 gäller avtalet på obestämd tid. En part får när som helst säga upp avtalet genom skriftligt meddelande till depositarien. En uppsägning träder för den uppsägande parten i kraft sex månader efter det att meddelande om uppsägning har lämnats. Om avtalet sägs upp, ska enligt stycke 9 säkerhetsskyddsklassificerade uppgifter eller material som har förmedlats under avtalet återsändas till den upprättande parten så snart som möjligt. Säkerhetsskyddsklassificerade uppgifter eller information som överlåtits under avtalet och som inte återlämnas ska trots uppsägning av avtalet även i fortsättningen skyddas i enlighet med föreskrifterna i avtalet. I stycke 10 anges de avtal och överenskommelser rörande skydd av säkerhetsskyddsklassificerade uppgifter som avtalet ersätter när det träder i kraft.

2 Lagförslag

I 95 § i grundlagen förutsätts att bestämmelser i internationella förpliktelser som hör till området för lagstiftningen sätts i kraft nationellt genom en särskild ikraftträdandelag. Sådana bestämmelser ska sättas i kraft genom en lag också när det till följd av förpliktelsen inte är nödvändigt att justera det materiella innehållet i den nationella lagstiftningen. Eftersom det inte är nödvändigt att ändra den materiella lagstiftningen för att genomföra förpliktelserna i säkerhetsskyddsavtalet mellan de nordiska länderna, innehåller propositionen endast ett förslag till blankettlag.

1 §. Genom bestämmelsen i lagförslagets 1 § sätts de bestämmelser i avtalet i kraft som hör till området för lagstiftningen. Dessa bestämmelser refereras nedan i avsnittet om riksdagens samtycke.

2 §. Om lagens ikraftträdande bestäms genom förordning av republikens president. Lagen avses träda i kraft samtidigt som avtalet träder i kraft för Finlands del.

Republikens president bemyndigas ytterligare i paragrafen att genom förordning bestämma att Finland meddelar att det börjar tillämpa avtalet i förhållande till de fördragsslutande stater som har lämnat ett likadant meddelande redan innan avtalet har trätt i kraft .

3 Ikraftträdande

Enligt artikel 14.1 i avtalet mellan Finland och de övriga nordiska länderna ska avtalsparterna deponera sina ratifikations-, godtagande- eller godkännandeinstrument hos Konungariket Norges regering. Avtalet träder i kraft trettio dagar efter det datum då ratifikations-, godtagande- eller godkännandeinstrumenten lämnats in av den sista av de regeringar som undertecknat avtalet.

Enligt artikel 14.3 i avtalet får varje part meddela att den anser sig vara bunden av avtalet i förhållande till någon annan part som har lämnat liknande meddelande. Dessa meddelanden träder ikraft trettio dagar efter dagen för mottagandet av meddelandet. Avsikten är att Finland lämnar ett sådant meddelande. Då skulle det vara möjligt att temporärt tillämpa bestämmelserna i avtalet i förhållande till andra fördragsslutande parter som har lämnat likadana meddelanden innan avtalet träder i kraft. Enligt preliminära uppgifter handlar det åtminstone om Sverige och Norge.

Lagen om sättande i kraft av avtalet avses träda i kraft samtidigt som avtalet för Finlands del träder i kraft vid en tidpunkt som bestäms genom förordning av republikens president.

Det generella säkerhetsskyddsavtalet ersätter vid ikraftträdandet överenskommelsen rörande säkerhetsskyddets utformning inom ramen för avtalet om nordiskt samarbete inom försvarsmaterielområdet mellan Danmark, Finland, Norge och Sverige.

I 2 § i ikraftträdandelagen bemyndigas republikens president att genom förordning bestämma att Finland meddelar att det börjar tillämpa avtalet i förhållande till de fördragsslutande stater som har lämnat ett likadant meddelande redan innan avtalet har trätt i kraft .

4 Behovet av riksdagens samtycke och behandlingsordning

4.1 Behovet av riksdagens samtycke

Enligt 94 § 1 mom. i grundlagen krävs riksdagens godkännande för fördrag och andra internationella förpliktelser som innehåller sådana bestämmelser som hör till området för lagstiftningen. Enligt grundlagsutskottets tolkningspraxis ska en bestämmelse anses höra till området för lagstiftningen om den gäller utövande eller begränsning av någon grundläggande fri- eller rättighet som är skyddad i grundlagen, om den i övrigt gäller grunderna för individens rättigheter och skyldigheter, om den sak som bestämmelsen gäller är sådan att om den enligt grundlagen ska föreskrivas i lag eller om det finns lagbestämmelser om den sak som bestämmelsen gäller eller om det enligt rådande uppfattning i Finland ska lagstiftas om saken. Enligt grundlagsutskottet hör en bestämmelse om en internationell förpliktelse på dessa grunder till området för lagstiftningen oavsett om den strider mot eller överensstämmer med en lagbestämmelse i Finland (se t.ex. GrUU 11/2000 rd och GrUU 12/2000 rd).

På de grunder som nämns ovan kräver flera bestämmelser i det avtal som ingår i propositionen riksdagens samtycke. I *artikel 1* föreskrivs om dess syfte och tillämpningsområde. I *artikel 2* definieras vad som avses med säkerhetsskyddsklassificerade uppgifter, upprättande part, mottagande part, säkerhetsskyddsklassificerade kontrakt, behörig säkerhetsmyndighet, kontraktstagare, säkerhetsöverträdelse, säkerhetsklarering, behörighet till säkerhetsskyddsklassificerade uppgifter och tredje part. Eftersom dessa bestämmelser i avtalet direkt eller indirekt påverkar tolkningen och tillämpningen av materiella bestämmelser som hör till området för lagstiftningen kräver de riksdagens godkännande (GrUU 6/2001 rd).

I *artikel 3.1* förutsätts det att parterna ska vidta lämpliga åtgärder, i enlighet med den egna nationella lagstiftningen, för att skydda de säkerhetsskyddsklassificerade uppgifter som avtalet omfattar och de åtar sig därigenom att skydda de säkerhetsskyddsklassificerade uppgifterna på samma nivå som egen information i motsvarande säkerhetsklass, vilket förutsätter att säkerhetsklassificerad information som tas emot förses med korrekt anteckning. I lagen om internationella förpliktelser som gäller informationssäkerhet föreskrivs om myndigheternas åtgärder för att genomföra dessa förpliktelser. I 8 § i lagen förpliktas myndigheten att förse särskilt känsligt informationsmaterial med anteckning om säkerhetsklass. Bestämmelsen hör till området för lagstiftningen.

Restriktioner angående yppande och användning av säkerhetsskyddsklassificerad information formuleras i *artikel 4*. I artikeln finns föreskrifter om skyldigheten att skydda säkerhetsskyddsklassificerad information inom avtalets tillämpningsområde med nationella åtgärder som begränsar förmedling, användning och tillgång till säkerhetsklassificerad information. Den mottagande parten får inte ge ut säkerhetsskyddsklassificerad information utan den upprättande partens tillstånd.

I Finland är myndighetshandlingar enligt huvudregeln offentliga. Var och en har enligt 12 § 2 mom. i grundlagen rätt att ta del av myndigheters offentliga handlingar. Denna rätt kan endast av tvingande skäl begränsas genom lag. Allmänt tillämpliga bestämmelser om sekretess- och klassificeringsanteckningar ingår i 25 § i offentlighetslagen. Enligt paragrafen ska anteckning om sekretess göras i handlingar som en myndighet ger ut till en part och som ska vara sekretessbelagda på grund av någon annans eller allmänt intresse. I andra sekretessbelagda handlingar kan en anteckning göras efter prövning.

Avvikande från bestämmelserna i offentlighetslagen ska särskilt känsligt informationsmaterial enligt 6 § 1 mom. i lagen om internationella förpliktelser som gäller informationssäkerhet i lydelsen av den 1 november 2010 (885/2010) sekretessbeläggas, om inte annat följer av en internationell förpliktelse som gäller informationssäkerhet. I propositionen motiverades ändringen med situationer som har framkommit vid avtalsförhandlingar som Finland fört, där en avtalspart inte garanterar ovillkorlig sekretess med stöd av avtalet, utan där frågan måste avgöras från fall till fall utgående från en sådan prövning av skaderekvisitet som baserar sig på den nationella lagstiftningen. Det är inte ändamålsenligt att Finland iakttar en mera omfattande sekretess än andra avtalsparter. Av denna anledning föreslogs det i propositionen att en bestämmelse tas in i 1 mom., enligt vilken sekretessen ska vara beroende av innehållet i respektive avtal eller annan internationell förpliktelse. Genom ändringen reserverar man sig för internationella avtal som behandlas senare, såsom det föreliggande avtalet mellan de nordiska länderna. Avtalsbestämmelsen är följaktligen i samklang med bestämmelserna i gällande 6 § 1 mom.

I 8 § i samma lag finns det bestämmelser om anteckning av säkerhetsklass i särskilt känsligt informationsmaterial. Enligt den ska särskilt känsligt informationsmaterial oberoende av vad som föreskrivs i lagen om offentlighet i myndigheternas verksamhet förses med sådan anteckning om säkerhetsklass som anges i en internationell förpliktelse som gäller informationssäkerhet, för att ange vilka säkerhetskrav som ska iakttas vid hanteringen av materialet. Bestämmelserna i avtalet ställer följaktligen strängare krav än offentlighetslagen i Finland på anteckning om sekretess i säkerhetsklassificerad information. Bestämmelserna kräver riksdagens samtycke. I artikel 4.3 punkt b föreskrivs det vidare om parternas skyldighet att göra en relevant säkerhetsutredning över personer som har tillgång till säkerhetsklassificerad information som avses i avtalet. I upplägget för säkerhetsutredningar ska det som sägs i 10 § 1 mom. i grundlagen om tryggat privatliv och om plikten att lagstifta om skydd för personuppgifter beaktas. I Finland finns det föreskrifter om personer som är föremål för säkerhetsutredningar samt om utredningsförfarandet i lagen om säkerhetsutredningar.

I *artikel 7* finns det bestämmelser om besök av fysiska personer från en fördragsslutande part till värdpartens lokaler, där det hanteras säkerhetsklassificerad information. Syftet med besök mellan de fördragsslutande parternas representanter är att säkerställa att avtalets syfte om ett korrekt skydd för säker-

hetsklassificerad information ska förverkligas. Denna besöksrätt innehåller inget sådant utövande av offentlig makt eller sådan granskningsrätt som står i konflikt med grundlagen (GrUU 179/1997). Genom avtalsbestämmelsen uppkommer det också indirekt en skyldighet för privata beställningsmottagare att tillåta besök i sina egna lokaler. I 18 § i lagen om internationella förpliktelser som gäller informationssäkerhet finns motsvarande föreskrifter om faktorer i anslutning till verkställandet av avtalets besöksbestämmelse.

I *artikel 8* finns det bestämmelser om säkerhetsskyddsklassificerade kontrakt och om de säkerhetsutredningar sådana kontrakt kräver. Föreskrifter om säkerhetsutredningar som gäller sammanslutningar ingår i 12 och 13 § i lagen om internationella förpliktelser om informationssäkerhet. Bestämmelsen ska alltså anses höra till området för lagstiftningen.

I artikel 9 finns bestämmelser om översättning, kopiering och förstöring av säkerhetsklassificerad information. Om arkivering av säkerhetsklassificerad information föreskrivs i arkivlagen. Bestämmelserna om kopiering av sådant material ingår däremot i 17 § i informationssäkerhetsförordningen och bestämmelserna om förstöring i 21 §. Till den delen kräver bestämmelserna följaktligen inte riksdagens samtycke. I *artikel 11* krävs det att en part utan dröjsmål ska meddela berörda fördragsslutande parter vid säkerhetsöverträdelser. Parterna är skyldiga att utreda säkerhetsöverträdelser som gäller säkerhetsklassificerad information och i mån av möjlighet att vidta åtgärder för att begränsa de konsekvenser som överträdelsen har medfört och förebygga ytterligare överträdelser samt vid behov bistå varandra i undersökningarna. I 19 § i lagen om internationella förpliktelser som gäller informationssäkerhet föreskrivs om de nationella säkerhetsmyndigheternas skyldigheter i sådana situationer som avses i avtalets bestämmelser.

4.2 Behandlingsordning

Bestämmelser som är av betydelse för behandlingsordningen ingår i artikel 4 i avtalet som innehåller restriktioner för offentligheten av information och material som har säkerhetsklassificerats. Avtalsbestämmelserna är av betydelse för rätten till information enligt offentlighetsprincipen som tryggas genom grundlagens 12 § 2 mom. Denna rätt till information får endast begränsas genom lag och av tvingande skäl. Att trygga Finlands och finländska företags möjligheter att delta på internationellt och nordiskt plan i bilaterala aktiviteter och projekt som kräver utbyte av känslig och sekretessbelagd information kan anses vara ett sådant tvingande skäl. I lagen om internationella förpliktelser som gäller informationssäkerhet ingår det en specialbestämmelse om sekretess i 6 §.

Säkerhetsskyddsavtalet om ömsesidigt skydd och utbyte av säkerhetsskyddsklassificerade uppgifter kan inte anses innehålla bestämmelser som berör grundlagen på det sätt som avses i 94 § 2 mom. och 95 § 2 mom. i grundlagen. Enligt regeringens uppfattning kan avtalet följaktligen godkännas med enkel majoritet och förslaget om sättande i kraft av de bestämmelser i avtalet som hör till området för lagstiftningen godkännas i vanlig lagstiftningsordning.

Med stöd av det som anförts ovan och i enlighet med grundlagens 94 § föreslås

> *att Riksdagen godkänner det i Oslo den 7 maj 2010 mellan Danmark, Norge, Sverige, Finland, och Island ingångna generella säkerhetsskyddsavtalet om ömsesidigt skydd och utbyte av säkerhetsskyddsklassificerade uppgifter.*

Eftersom avtalet innehåller bestämmelser som hör till området för lagstiftningen överlämnas samtidigt följande lagförslag till riksdagen:

Lagförslag

Lag

om sättande i kraft av de bestämmelser som hör till området för lagstiftningen i det generella säkerhetsskyddsavtalet mellan Danmark, Finland, Island, Norge och Sverige

I enlighet med riksdagens beslut föreskrivs:

1 §

De bestämmelser som hör till området för lagstiftningen i det i Oslo den 7 maj 2010 mellan Danmark, Finland, Island, Norge och Sverige upprättade avtalet om ömsesidigt skydd och utbyte av säkerhetsskyddsklassificerade uppgifter gäller som lag sådana Finland har förbundit sig till dem.

2 §

Om ikraftträdandet av denna lag bestäms genom förordning av republikens president. Genom förordning av republikens president får bestämmas att denna lag tillämpas innan avtalet träder i kraft i förhållande till de avtalsparter som har meddelat eller kommer att meddela att de tillämpar avtalet innan det träder i kraft i förhållande till de fördragsslutande parter som har lämnat ett likadant meddelande.

Helsingfors den 5 november 2010

Republikens President

TARJA HALONEN

Utrikesminister *Alexander Stubb*

Fördragstext

GENERELLT SÄKERHETSSKYDDS-AVTAL OM ÖMSESIDIGT SKYDD OCH UTBYTE AV SÄKERHETSSKYDDS-KLASSIFICERADE UPPGIFTER

MELLAN

DANMARK,
FINLAND,
ISLAND,
NORGE
OCH
SVERIGE

Konungariket Danmarks regering, Republiken Finlands regering, Islands regering, Konungariket Norges regering och Konungariket Sveriges regering, nedan kallade parterna, har - i syfte att skydda säkerhetsskyddsklassificerade uppgifter i direkt utbyte, eller i utbyte mellan andra offentliga eller privata organisationer eller juridiska personer som hanterar säkerhetsskyddsklassificerade uppgifter inom parternas respektive jurisdiktion kommit överens om följande.

Artikel 1

Syfte och tillämpning

(1) Syftet med detta avtal är att skydda de säkerhetsskyddsklassificerade uppgifter som utbyts mellan två eller flera av parterna, eller mellan kontraktsparter inom parternas respektive jurisdiktion, inom utrikes-, försvars-, säkerhets-, polis- eller företagssamarbete, eller som framtagits grundade på, eller som härrör från, de uppgifter som har utbytts.

(2) Detta avtal får inte åberopas av en part i syfte att få tillgång till uppgifter som en annan part har mottagit från en tredje part.

GENERAL SECURITY AGREEMENT ON THE MUTUAL PROTECTION AND EXCHANGE OF CLASSIFIED INFORMATION

BETWEEN

DENMARK,
FINLAND,
ICELAND,
NORWAY
AND
SWEDEN

The Government of the Kingdom of Denmark, the Government of the Republic of Finland, the Government of Iceland, the Government of the Kingdom of Norway and the Government of the Kingdom of Sweden, hereafter called the Parties, in order to safeguard any Classified Information exchanged directly or through other State bodies or public or private legal entities that deal with Classified Information under the jurisdiction of the Parties, have agreed upon the following:

Article 1

Purpose and scope of application

(1) The purpose of this Agreement is to protect Classified Information exchanged between two or more of the Parties, or between Contractors under the jurisdiction of the Parties, in the areas of foreign affairs, defence, security, police or scientific, industrial and technological cooperation, or produced on the basis of, or arising from, exchanged information.

(2) This Agreement may not be invoked by a Party in order to obtain Classified Information that other Parties have received from a Third Party.

Artikel 2

Definitioner

(1) I detta avtal avses med:
Säkerhetsskyddsklassificerade uppgifter
Information, oavsett form, som enligt parternas lagstiftning kräver skydd mot förlust, obehörig åtkomst eller annat röjande och har märkts som sådan;

Upprättande part
En part, liksom statliga organ eller offentliga och privata organisationer inom dess jurisdiktion, som delger säkerhetsskyddsklassificerad information;
Mottagande part
En part, liksom statliga organ eller offentliga och privata organisationer under dess jurisdiktion, till vilken säkerhetsskyddsklassificerad information är delgiven av en upprättande part;
Säkerhetsskyddsklassificerat kontrakt
Ett kontrakt som innehåller eller avser säkerhetsskyddsklassificerade uppgifter;
Behörig säkerhetsmyndighet
En statlig myndighet som ansvarar för säkerhetsfrågor;
Kontraktstagare
En fysisk eller juridisk person med rättslig förmåga att ingå kontrakt;
Säkerhetsöverträdelse
En gärning eller försummelse som bryter mot nationella säkerhetsregler och som kan medföra att säkerhetsskyddsklassificerade uppgifter äventyras eller röjs;
Säkerhetsklarering
Ett positivt utfall av prövning av en persons eller ett företags lämplighet att ges tillgång till och handha säkerhetsskyddsklassificerade uppgifter på viss nivå i enlighet med respektive lands säkerhetsbestämmelser;

"Behörighet till säkerhetsskyddsklassificerade uppgifter"
En princip som enligt vilken tillgång till säkerhetsskyddsklassificerade uppgifter endast får ges till personer i samband med officiella uppdrag och uppgifter;
Tredje part
En institution, internationell eller nationell organisation, enhet eller stat som inte är part i detta avtal.

Article 2

Definitions

(1) For the purpose of this Agreement:
Classified Information means
information, regardless of its form, that under the laws of either Party requires protection against loss, unauthorised disclosure or other compromise and has been so designated;
Originating Party means
the Party, as well as any other State bodies or public or private legal entities under its jurisdiction, releasing Classified Information;

Receiving Party means
the Party, as well as any other State bodies or public or private legal entities under its jurisdiction, to which Classified Information is released by the Originating Party;

Classified Contract means
a contract which contains or involves Classified Information;
Competent Security Authority means
any Government authority responsible for security issues;
Contractor means
an individual or a legal entity possessing the legal capability to undertake contracts;
Breach of Security means
an act or an omission contrary to national security regulations the result of which may endanger or compromise Classified Information;
Security Clearance means
a positive determination following an investigative procedure to ascertain the eligibility of a person or entity to have access to and to handle Classified Information on a certain level in accordance with the relevant national security regulations;
"Need to Know" means

a principle by which access to Classified Information may only be granted to individuals in connection with their official duties or tasks;
Third Party means
any institution, international or national organisation, legal entity or State that is not a Party to this Agreement.

En part i detta avtal betraktas som "Tredje part" i samband med samarbete i vilket parten inte deltar.

A Party to this Agreement is considered as a “Third Party” regarding co-operation activities in which the Party does not participate.

Artikel 3

Skydd av säkerhetsskyddsklassificerade uppgifter

(1) Parterna ska vidta lämpliga åtgärder, i enlighet med den egna nationella lagstiftningen, för att skydda de säkerhetsskyddsklassificerade uppgifter som avtalet omfattar. Parterna ska se till att de säkerhetsskyddsklassificerade uppgifter som detta avtal omfattar får samma nivå av säkerhetsskydd som ges för egna säkerhetsskyddsklassificerade uppgifter i motsvarande informationssäkerhetsklass, enligt definitionen i Artikel 5.

(2) Tillgång till säkerhetsskyddsklassificerade uppgifter på nivån CONFIDENTIAL eller högre, och tillträde till platser och anläggningar där säkerhetsskyddsklassificerade uppgifter förvaras eller där verksamhet bedrivs i vilken säkerhetsskyddsklassificerade uppgifter förekommer, ska begränsas till dem som har säkerhetsklarerats och som har behörighet till säkerhetsskyddsklassificerade uppgifter.

(3) Parterna ska inom ramen för detta avtal ömsesidigt erkänna varandras säkerhetsklareringar.

(4) Varje part ska se till att säkerhetslagstiftning, säkerhetsföreskrifter och säkerhetspraxis följs vid de myndigheter, företag och anläggningar, inom den egna jurisdiktionen, som äger, utvecklar, framställer och/eller använder de andra parternas säkerhetsskyddsklassificerade uppgifter.

Article 3

Protection of Classified Information

(1) The Parties shall take appropriate measures, in accordance with their national legislation, to protect Classified Information under this Agreement. The Parties shall afford to all Classified Information under this Agreement the same degree of security protection as is provided to their own Classified Information of equivalent level of classification, as defined in Article 5.

(2) Access to Classified Information on the level CONFIDENTIAL or above, and to locations and facilities where Classified Information is stored or activities involving Classified Information are performed, shall be limited to those who have been granted a Security Clearance and who have a Need to Know.

(3) Within the framework of this Agreement the Parties shall mutually recognise each others' Security Clearances.

(4) Each Party shall supervise the observance of security laws, regulations and practices at agencies, offices and facilities within their jurisdiction that possess, develop, produce and/or use Classified Information of other Parties.

Artikel 4

Delgivning och användning av säkerhetsskyddsklassificerad information

(1) Principen om upprättande parts medgivande ska respekteras av parterna i enlighet med deras konstitutionella bestämmelser, nationella lagar och andra författningar och säkerhetsskyddsklassificerade uppgifter, som omfattas av detta avtal, får inte delges tredje part eller medborgare i andra länder utan fö-

Article 4

Disclosure and use of Classified Information

(1) The Parties shall respect the principle of originator consent in accordance with their constitutional requirements, national laws and regulations, and not disclose Classified Information under this Agreement to Third Parties or nationals of other countries without prior written consultation with the Originat-

regående skriftligt samråd med upprättande part. Säkerhetsskyddsklassificerade uppgifter som mottagits av någon av parterna från en annan part ska endast användas för det syfte som angetts.

(2) I det fall en part eller tillhörande myndigheter eller organisationer inom de områden som anges i Artikel 1, tilldelar kontrakt för verksamhet i annan parts land, och om kontraktet omfattar säkerhetsskyddsklassificerade uppgifter, så är det parten i det land i vilket den avtalade verksamheten äger rum, som ansvarar för hantering av sådana säkerhetsskyddsklassificerade uppgifter i enlighet med dess egna regler och krav.

(3) Mottagande part ska, innan delgivning av säkerhetsskyddsklassificerade uppgifter som har mottagits av annan part eller kontraktstagare eller möjliga kontraktstagare inom partens jurisdiktion:

a. Säkerställa att sådana kontraktstagare eller möjliga kontraktstagare och deras anläggningar har möjlighet att ge de säkerhetsskyddsklassificerade uppgifterna adekvat skydd.

b. Se till att lämplig säkerhetsklarering finns för berörda kontraktstagares anläggningar och för all den personal som i sin tjänst behöver säkerhetsskyddsklassificerade uppgifter.

c. Säkerställa att personer som har tillgång till säkerhetsskyddsklassificerade uppgifter har upplysts om deras skyldighet att skydda de säkerhetsskyddsklassificerade uppgifterna i enlighet med tillämplig lagstiftning.

d. Utföra regelbundna säkerhetsskyddskontroller vid berörda klarerade anläggningar.

Artikel 5

Informationssäkerhetsklasser

(1) Säkerhetsskyddsklassificerade uppgifter ska förses med någon av följande beteckningar för informationssäkerhetsklasser.

ing Party. Classified Information released by one Party to other Parties shall be used for the specified purpose only.

(2) In the event that a Party and/or its agencies or entities concerned with subjects set out in Article 1 award a contract for performance within the territory of one of the other Parties and such contract involves Classified Information, the Party of the country in which the performance under the contract is to take place shall assume responsibility for administering such Classified Information in accordance with its own standards and requirements.

(3) The Receiving Party, prior to the release of any Classified Information received from other Parties to Contractors or prospective Contractors under its jurisdiction, shall:

a. ensure that such Contractors or prospective Contractors and their facilities have the capability to protect the Classified Information adequately;

b. grant an appropriate Security Clearance to the relevant Contractor's facilities and to all its personnel whose duties require access to the Classified Information;

c. ensure that all persons having access to the Classified Information are informed of their responsibilities to protect the Classified Information in accordance with the applicable laws;

d. carry out periodic security inspections of relevant security cleared facilities.

Article 5

Security classifications

(1) Classified Information shall be marked with one of the following security classification levels:

Engelsk översättning	"TOP SECRET"	"SECRET"	"CONFIDENTIAL"	"RESTRICTED"
DENMARK	YDERST HEMMELIGT	HEMMELIGT	FORTROLIGT	TIL TJENESTEBRUG
FINLAND	ERITTÄIN SALAINEN / YTTERST HEMLIG	SALAINEN/ HEMLIG	LUOTTA-MUKSELLINEN/ KONFIDENTIELL	KÄYTTÖ RAJOITETTU/ BEGRÄNSAD TILLGÅNG
ICELAND	ALGJORT LEYNDARMAL	LEYNDARMAL	TRUNADARMAL	TAKMARKADUR ADGANGUR
NORWAY	STRENGT HEMMELIG	HEMMELIG	KONFIDENSIELT	BEGRENSET
SWEDEN FÖRSVARS-MYNDIGHETER ÖVRIGA MYNDIGHETER	HEMLIG/ TOP SECRET	HEMLIG/ SECRET	HEMLIG/ CONFIDENTIAL	HEMLIG/ RESTRICTED
	HEMLIG AV SYNNERLIG BETYDELSE FÖR RIKETS SÄKERHET	HEMLIG	-	-

(2) Mottagande part och/eller dess myndigheter eller organisationer får inte ändra informationssäkerhetsklass på de säkerhetsskyddsklassificerade uppgifter som mottagits, utan att detta har föregåtts av upprättande parts skriftliga medgivande. Upprättande part ska informera mottagande part om förändringar som görs i informationssäkerhetsklassning av den information som har utbytts.

(3) Mottagande part ska förse de säkerhetsskyddsklassificerade uppgifter som har mottagits med den egna beteckningen för motsvarande informationssäkerhetsklass. Översättningar och kopior ska förses med beteckning för samma informationssäkerhetsklass som originalet.

(2) The Receiving Party and/or its agencies or entities shall not change the security classification level of received Classified Information without the prior written consent of the Originating Party. The Originating Party shall inform the Receiving Party of any changes in the security classification of the exchanged information.

(3) The Receiving Party shall mark the received Classified Information with its own equivalent security classification level. Translations and reproductions shall be marked with the same security classification level as the original.

(4) Uppgifter från Sverige som endast har beteckningen "HEMLIG" ska betraktas som HEMLIG/SECRET.

Artikel 6

Behöriga säkerhetsmyndigheter och säkerhetssamarbete

(1) De behöriga säkerhetsmyndigheterna ska övervaka genomförandet av detta avtal.

(2) Parterna ska meddela varandra om vilka säkerhetsmyndigheter som är behöriga och om förändringar görs i detta avseende.

(3) För att åstadkomma och upprätthålla jämförbara säkerhetsstandarder ska de behöriga säkerhetsmyndigheterna på begäran förse varandra med information rörande deras nationella lagstiftning, standarder, metoder och praxis för skydd av säkerhetsskyddsklassificerade uppgifter. För att uppnå detta mål får de behöriga säkerhetsmyndigheterna besöka varandra.

(4) De behöriga säkerhetsmyndigheterna ska informera varandra om alla relevanta säkerhetshot som kan äventyra delgivna säkerhetsskyddsklassificerade uppgifter.

(5) De behöriga säkerhetsmyndigheterna ska på begäran, i enlighet med nationell lagstiftning, bistå varandra med att genomföra säkerhetsklareringsärenden.

(6) De behöriga säkerhetsmyndigheterna ska skyndsamt informera varandra om förändringar i ömsesidigt erkända säkerhetsklareringar.

(7) Parternas underrättelse- och säkerhetstjänster får, i enlighet med nationell lagstiftning, utbyta operativ och/eller underrättelseinformation direkt mellan dem.

Artikel 7

Besök

(1) Besök som medför tillgång till säkerhetsskyddsklassificerade uppgifter på nivån CONFIDENTIAL eller högre, eller till områden där sådana säkerhetsskyddsklassificerade uppgifter tas eller kan tas fram, handhas eller lagras, kräver ett föregående skriftligt tillstånd från den behöriga säkerhetsmyndighe-

(4) Information from Sweden bearing the sole marking "HEMLIG" shall be regarded as HEMLIG/SECRET.

Article 6

Competent Security Authorities and Security Cooperation

(1) The Competent Security Authorities shall supervise the implementation of this Agreement.

(2) The Parties shall notify each other of the designation of their Competent Security Authorities and any changes thereto.

(3) In order to achieve and maintain comparable standards of security, the Competent Security Authorities shall, on request, provide each other with information about their national laws and regulations, standards, procedures and practices for the protection of Classified Information. To this aim the Competent Security Authorities may visit each other.

(4) The Competent Security Authorities shall inform each other of any relevant security risks that may endanger released Classified Information.

(5) On request, the Competent Security Authorities shall, in accordance with national legislation, assist each other in carrying out Security Clearance procedures.

(6) The Competent Security Authorities shall promptly inform each other about any changes in mutually recognized Security Clearances.

(7) The intelligence and security services of the Parties may, in accordance with national legislation, exchange operative and/or intelligence information directly with each other.

Article 7

Visits

(1) Visits entailing access to Classified Information classified as CONFIDENTIAL or above, or to areas where such Classified Information is or may be developed, handled or stored, require a prior written authorization from the Competent Security Authority of the host Party receiving the visitors.

ten hos den mottagande parten som tar emot besökare.

(2) Behörighet att ta del av säkerhetsskyddsklassificerade uppgifter och tillträde till anläggningar och lokaler där verksamhet som säkerhetsskyddsklassificerade uppgifter bedrivs eller där säkerhetsskyddsklassificerade uppgifter förvaras eller hanteras ska endast medges av den mottagande parten till besökare om de har:

a. Säkerhetsklarerats av behörig säkerhetsmyndighet eller annan behörig statlig myndighet i den avsändande parten och de är behöriga att ta del av säkerhetsskyddsklassificerade uppgifter i enlighet med värdlandets nationella lagar och regler, eller

b. Getts behörighet av behörig säkerhetsmyndighet eller annan behörig statlig myndighet i respektive land att genomföra nödvändiga besök.

(3) Behörig säkerhetsmyndighet hos den part som gör förfrågan ska meddela behörig säkerhetsmyndighet hos den part som besöket planeras till, i enlighet med denna artikels bestämmelser, och ska säkerställa att den senare har mottagit besöksförfrågan senast 10 arbetsdagar innan besöket ska äga rum. I brådskande fall får de behöriga säkerhetsmyndigheterna komma överens om en kortare tidsperiod.

(4) Besöksförfrågan ska innehålla:

a. Besökarens för- och efternamn, födelseort och -datum, nationalitet, befattning och arbetsgivare, en beskrivning av vilket projekt som besökaren deltar i, pass- eller idnummer.

b. En försäkran om besökarens säkerhetsklarering i överensstämmelse med besökets syfte.

c. Syftet med besöket eller besöken, inkluderande den högsta nivån av säkerhetsskyddsklassificerade uppgifter som berörs.

d. Det begärda besökets eller besökens planerade tidpunkt och längd. I fallet med återkommande möten ska om möjligt hela periodens möten anges.

e. Namn, adress, telefon- och faxnummer, e-postadress och kontaktperson vid den anläggning som ska besökas, tidigare kontakter samt annan information av vikt för att avgöra behovet av besöket eller besöken.

(2) Access to Classified Information and to establishments and facilities where activities involving Classified Information are performed, or where Classified Information is stored or handled, shall be allowed by the host Party to visitors only if they have been:

a. security cleared by the Competent Security Authority or other competent government authority of the sending Party and are authorized to receive Classified Information in accordance with the national laws and regulations of the host Party, and/or

b. authorized by the Competent Security Authority or other competent government authority of the host Party to perform the required visit or visits.

(3) The Competent Security Authority of the requesting Party shall notify the relevant Competent Security Authority of the host Party of the planned visit in accordance with the provisions laid down in this Article, and shall make sure that the latter receives the visit request at least 10 working days before the visit takes place. In urgent cases the Competent Security Authorities may agree on a shorter period.

(4) The visit request shall include:

a. the visitor's surname, name, place and date of birth and nationality, the visitor’s position, with a specification of the employer which the visitor represents, a specification of the project in which the visitor participates, the visitor's passport number or other identity document number;

b. confirmation of the visitor's Security Clearance in accordance with the purpose of the visit;

c. the purpose of the visit or visits, including the highest level of Classified Information to be involved;

d. the expected date and duration of the requested visit or visits. In the case of recurring visits the total period covered by the visits shall be stated, when possible;

e. the name, address, phone/fax number, e-mail and point of contact of the establishment/facility to be visited, previous contacts and any other information useful to determine the justification of the visit or visits;

f. Datum och signatur eller stämpel av den sändande behöriga säkerhetsmyndigheten.

(5) Besöksförfrågan ska göras i enlighet med de principer som har överenskommits av de behöriga säkerhetsmyndigheterna.

(6) Giltigheten för besöksbehörigheten får inte överstiga tolv (12) månader.

(7) Den mottagande parten får, om det är nödvändigt, kräva ett certifikat över säkerhetsklarering.

(8) Andra besöksrutiner får tillämpas om parternas respektive säkerhetsmyndighet har kommit överens om det.

f. the date and signature or stamp of the sending Competent Security Authority.

(5) The visit request shall be submitted in accordance with principles agreed upon by the relevant Competent Security Authorities.

(6) The validity of authorizations for recurring visits shall not exceed twelve (12) months.

(7) The host Party may, if necessary, request a Security Clearance Certificate.

(8) Other visit procedures may be used if mutually agreed between the Competent Security Authorities of the relevant Parties.

Artikel 8

Säkerhetsskyddsklassificerade kontrakt

(1) Behörig säkerhetsmyndighet för den part som vill sluta säkerhetsskyddsklassificerat kontrakt med kontraktstagare i annan parts land får på förhand begära en säkerhetsklarering (eller motsvarande) som utfärdats för den aktuella kontraktstagarens anläggningar av den andra partens behöriga säkerhetsmyndighet. Om kontraktstagaren saknar en säkerhetsklarering, får den part som vill sluta ett säkerhetsskyddsklassificerat kontrakt begära av den part som kontraktstagaren tillhör att en säkerhetsklarering (eller motsvarande) utfärdas i enlighet med nationella lagar och bestämmelser.

(2) Om det sker en öppen anbudsgivning får den mottagande partens behöriga säkerhetsmyndighet tillhandahålla relevanta säkerhetscertifikat till den upprättande partens behöriga säkerhetsmyndighet utan en formell begäran.

(3) Ett säkerhetsskyddsklassificerat kontrakt ska innehålla tillämpliga säkerhetsbestämmelser och kompletteras med dokumentation som identifierar den information eller de beståndsdelar eller förhållanden som är säkerhetsskyddsklassificerade i kontraktet.

(4) Behörig säkerhetsmyndighet för den part som tecknar kontraktet ska säkerställa att kopior av all tillämplig säkerhetsrelaterad dokumentation som berör det säkerhetsskyddsklassificerade kontraktet kommer den behöriga säkerhetsmyndigheten i det land där kontraktet ska utföras tillhanda.

Article 8

Classified Contracts

(1) Prior to placing a Classified Contract within the country of any other Party, the Competent Security Authority of a Party may request a Security Clearance (or equivalent) issued to the facility of the Contractor in question by the Competent Security Authority of the other Party. If the Contractor does not possess a Security Clearance, the Party placing the Classified Contract may request the Party of the Contractor to issue a Security Clearance (or equivalent) in accordance with national laws and regulations.

(2) In the case of an open tender the Competent Security Authority of the Receiving Party may provide the Competent Security Authority of the Originating Party with the relevant security certificates without a formal request.

(3) A Classified Contract shall contain appropriate security provisions and be supplemented with documentation identifying the information or those elements or aspects of the Contract which are classified.

(4) The Competent Security Authority of the Party placing the Classified Contract shall ensure that copies of all relevant security documents in relation to the Contract are forwarded to the Competent Security Authority in whose country the Contract is to be implemented.

Artikel 9

Översättning, reproduktion och förstöring av säkerhetsskyddsklassificerade uppgifter

(1) Alla reproduktioner och översättningar ska vara försedda med tillämplig märkning av säkerhetsskyddsklassificering och skyddas som den säkerhetsskyddsklassificerade originalinformationen. Översättningarna och reproduktionerna ska begränsas till ett minimum som är nödvändigt för ett officiellt syfte.

(2) Alla översättningar ska innehålla en anteckning på det översatta språket som visar att de innehåller säkerhetsskyddsklassificerade uppgifter från den upprättande parten.

(3) Säkerhetsskyddsklassificerad information som markerats TOP SECRET får endast översättas eller reproduceras efter ett skriftligt tillstånd från den upprättande parten.

(4) Säkerhetsskyddsklassificerad information som markerats TOP SECRET får inte förstöras utan föregående skriftligt samtycke av den upprättande parten. Den ska återlämnas till den upprättande parten efter det att den inte längre bedöms nödvändig av de relevanta parterna.

(5) Information som klassificerats som SECRET ska förstöras av den mottagande staten i enlighet med nationella lagar och bestämmelser efter det att den inte längre bedöms nödvändig.

(6) Om en krissituation omöjliggör att säkerhetsskyddsklassificerade uppgifter kan skyddas ska de omedelbart förstöras. Den mottagande parten ska så snart som möjligt meddela den behöriga säkerhetsmyndigheten i den upprättande parten om förstöringen av de säkerhetsskyddsklassificerade uppgifterna.

Article 9

Translation, reproduction and destruction of Classified Information

(1) All reproductions and translations shall bear appropriate security classification markings and be protected as the original Classified Information. The translations and the number of reproductions shall be limited to the minimum required for an official purpose.

(2) All translations shall contain a suitable annotation, in the language of translation, indicating that they contain Classified Information of the Originating Party.

(3) Classified Information marked TOP SECRET shall be translated or reproduced only upon the written permission of the Originating Party.

(4) Classified Information marked TOP SECRET shall not be destroyed without the prior written consent of the Originating Party. It shall be returned to the Originating Party after it is no longer considered necessary by the relevant Parties.

(5) Information classified as SECRET or below shall be destroyed after it is no longer considered necessary by the Receiving Party, in accordance with the national laws and regulations.

(6) If a crisis situation makes it impossible to protect Classified Information transferred under this Agreement, the Classified Information shall be destroyed immediately. The Receiving Party shall notify the Competent Security Authority of the Originating Party about the destruction of the Classified Information as soon as possible.

Artikel 10

Överföring av säkerhetsskyddsklassificerade uppgifter

(1) Säkerhetsskyddsklassificerade uppgifter ska i normala fall förmedlas mellan parterna med diplomatpost eller kurirer om inte de relevanta behöriga säkerhetsmyndigheterna kommit överens om annat.

Article 10

Transfer of Classified Information

(1) Classified Information shall normally be transferred between the Parties by using diplomatic channels or couriers, unless otherwise agreed by the relevant Competent Security Authorities.

(2) Om någon av parterna önskar överföra säkerhetsskyddsklassificerad information utanför sitt territorium ska en sådan överföring koordineras innan överföringen med den upprättande parten.

Artikel 11

Säkerhetsöverträdelser

(1) När en säkerhetsöverträdelse som inbegriper förlust eller röjande av säkerhetsskyddsklassificerade uppgifter som omfattas av detta avtal, ska behörig säkerhetsmyndighet i de land där säkerhetsöverträdelsen sker informera berörda parters säkerhetsmyndigheter så snart som möjligt.

(2) Den part som har jurisdiktion ska vidta vederbörliga åtgärder som är tillåtna enligt nationell lagstiftning för att begränsa de konsekvenser som säkerhetsöverträdelsen har medfört och förebygga ytterligare säkerhetsöverträdelser eller skador.

(3) Övriga berörda parter ska på begäran bistå utredningen. Övriga berörda parter ska alltid informeras om utredningens resultat och de åtgärder som har vidtagits till följd av säkerhetsöverträdelsen och ska i ett slutligt yttrande underrättas om skälen till och omfattningen av säkerhetsöverträdelsen, samt erhålla information om vilka åtgärder som vidtagits för att undvika upprepning.

Artikel 12

Kostnader

Kostnader för parterna inom ramen för detta avtal ska inte ersättas parterna emellan.

Artikel 13

Tvistlösning

Tvister om tolkningen eller tillämpningen av detta avtal ska lösas genom samråd parterna emellan och inte hänskjutas till nationell eller internationell domstol eller tredje part för avgörande.

(2) If one of the Parties wishes to transfer Classified Information outside its territory, such transfer shall be subject to prior coordination with the Originating Party.

Article 11

Breach of Security

(1) In case of a Breach of Security involving loss or unauthorized disclosure of Classified Information under this Agreement, the Competent Security Authority in whose country the Breach of Security occurs shall inform the Competent Security Authorities of the Parties concerned as soon as possible.

(2) The Party with jurisdiction shall undertake all appropriate measures possible under its national law so as to limit the consequences of the Breach of Security and to prevent further breaches or compromises.

(3) Upon request, the other Parties concerned shall provide investigative assistance. In any case, the other Parties concerned shall be informed of the results of the investigation and of the measures undertaken as a result of the Breach of Security, and shall receive a final statement as to the reasons and extent of the Breach of Security, and the measures adopted to prevent reoccurrences.

Article 12

Expenses

Expenses incurred by the Parties with respect to this Agreement shall not be subject to reimbursement between the Parties.

Article 13

Dispute settlement

Any dispute regarding the interpretation or application of this Agreement shall be resolved by consultation between the Parties and shall not be referred to any national or international tribunal or Third Party for settlement.

Artikel 14

Slutbestämmelser

(1) Detta avtal är föremål för ratifikation, godtagande eller godkännande. Ratifikations-, godtagande- eller godkännandeinstrumenten ska lämnas till Konungariket Norges regering, som härmed utses till depositarie.

(2) Detta avtal träder i kraft trettio (30) dagar efter det datum då ratifikations-, godtagande- eller godkännandeinstrumenten lämnats in av den sista av de regeringar som undertecknat avtalet.

(3) Fram till att avtalet träder i kraft får varje part då den lämnar sitt ratifikations-, godtagande- eller godkännandeinstrument eller vid en senare tidpunkt meddela att den anser sig vara bunden av avtalet i förhållande till någon annan part som har lämnat liknande meddelande. Dessa meddelanden träder ikraft trettio (30) dagar efter dagen för mottagandet av meddelandet.

(4) Ändringar av detta avtal får när som helst göras skriftligen förutsatt att samtliga parter godkänner ändringen.

(5) Ändringar som gjorts i enlighet med punkt 4 träder i kraft den trettionde (30) dagen efter det att samtliga parter har meddelat depositarien sitt godkännande.

(6) När detta avtal har trätt i kraft är det öppet för anslutning av tredje stat efter undertecknande regeringars godkännande. Anslutningsinstrumenten ska lämnas till Norges regering.

(7) För varje anslutande stat ska detta avtal träda i kraft på den trettionde (30) dagen efter det att sådan stat lämnat sitt anslutningsinstrument.

(8) Detta avtal gäller på obestämd tid. En part får, när som helst, säga upp avtalet genom skriftligt meddelande till depositarien. En sådan uppsägning träder i kraft för uppsägande part sex (6) månader efter det att meddelande om uppsägning har lämnats.

(9) Om avtalet sägs upp, ska säkerhetsskyddsklassificerade uppgifter eller föremål

Article 14

Final provisions

(1) This Agreement is subject to ratification, acceptance or approval. The instruments of ratification, acceptance or approval shall be deposited with the Government of the Kingdom of Norway, which is hereby designated as the Depositary.

(2) This Agreement shall enter into force on the thirtieth (30) day following the date of deposit of the instruments of ratification, acceptance or approval by the last signatory Government.

(3) Until the entry into force of this Agreement, each Party may notify at the time of the deposit of the instrument of ratification, acceptance or approval, or at any other subsequent time, that it shall consider itself bound by the Agreement in its relations with any other Party having made the same notification. These notifications shall take effect thirty (30) days after the date of receipt of the notification.

(4) Amendments to this Agreement may be made in writing at any time with the consent of all the Parties.

(5) Any amendment adopted in accordance with Paragraph 4 shall enter into force on the thirtieth (30) day after the last Party has informed the Depositary of its acceptance of the amendment.

(6) After the entry into force of this Agreement it shall be open to accession by third states upon consent of the signatory Governments. The instruments of accession shall be deposited with the Government of the Kingdom of Norway.

(7) For each acceding State this Agreement shall enter into force on the thirtieth (30) day following the date of deposit by such State of its instruments of accession.

(8) This Agreement shall be in force for an unlimited period of time. Any Party may, at any time, denounce the Agreement by means of a written notification to the Depositary. Such denunciation shall take effect with respect to the denouncing Party six (6) months after the date of deposit of the notification of denunciation.

(9) In the event of denunciation, Classified Information and/or items transmitted under

som har förmedlats under detta avtal återsändas till upprättande part så snart som möjligt. Säkerhetsskyddsklassificerade uppgifter eller information som inte återlämnas ska även i fortsättningen skyddas i enlighet med föreskrifterna i detta avtal.

(10) Vid ikraftträdandet ska detta avtal ersätta följande avtal och överenskommelser rörande skydd av säkerhetsskyddsklassificerade uppgifter mellan parterna:

1. ”Overenskomst mellom Kongeriket Sveriges regjering og Kongeriket Norges regjering vedrørende utveksling av militære informasjoner og materiell”/”Överenskommelse mellan Konungariket Sveriges regering och Konungariket Norges regering rörande visst utbyte av militära informationer och materiel”. Stockholm den 19 mai/maj 1969,

2. ”Sikkerhetdsaftale. Overenskomst vedrørende sikkerhedsaftalens udforming inden for rammeaftalen omfattende nordisk samarbejde inden for forsvarsmaterielområdet mellem Danmark, Finland, Norge og Sverige”/”Turvallisuussuojasopimus. Pohjoismaisen puolustusmateriaalialan yhteistyösopimuksen puitteissa laadittu turvallisuussuojaa koskeva yhteisymmärrys Tanskan, Suomen, Norjan ja Ruotsin välillä”/”Sikkerhetsavtale. Overenskomst om sikkerhetstiltakenes utforming innenfor rammen av avtalen om nordisk samarbeid på forsvarsmateriellområdet mellom Danmark, Finland, Norge og Sverige”/“Säkerhetsskyddsavtal. Överenskommelse rörande säkerhetsskyddets utformning inom ramen för avtalet om nordisk samarbete inom försvarsmaterielområdet mellan Danmark, Finland, Norge och Sverige“. 1994/1995.

Säkerhetsskyddsklassificerad information som utbytts i enlighet med de ovan nämnda avtalet och överenskommelserna ska även i fortsättningen vara skyddad enligt detta avtal.

Detta avtal är upprättat i ett original på de, danska, finska, isländska, norska, svenska och engelska språken. I händelse av tolkningsskiljaktighet ska den engelska texten gälla. Det undertecknade originalet ska deponeras i arkivet vid Konungariket Norges utrikesdepartement. Konungariket Norges utrikesdepartement ska sända bestyrkta kopior till parterna.

the terms of this Agreement shall be returned to the Originating Party as soon as possible. Classified Information and/or items that are not returned shall continue to be protected in accordance with the provisions of this Agreement.

(10) When entering into force, this Agreement replaces the following Agreements and Arrangements concerning the protection of Classified Information between the Parties:

1. ”Overenskomst mellom Kongeriket Sveriges regjering og Kongeriket Norges regjering vedrørende utveksling av militære informasjoner og materiell”/”Överenskommelse mellan Konungariket Sveriges regering och Konungariket Norges regering rörande visst utbyte av militära informationer och materiel”. Stockholm den 19 mai/maj 1969,

2. ”Sikkerhetdsaftale. Overenskomst vedrørende sikkerhedsaftalens udforming inden for rammeaftalen omfattende nordisk samarbejde inden for forsvarsmaterielområdet mellem Danmark, Finland, Norge og Sverige”/”Turvallisuussuojasopimus. Pohjoismaisen puolustusmateriaalialan yhteistyösopimuksen puitteissa laadittu turvallisuussuojaa koskeva yhteisymmärrys Tanskan, Suomen, Norjan ja Ruotsin välillä”/”Sikkerhetsavtale. Overenskomst om sikkerhetstiltakenes utforming innenfor rammen av avtalen om nordisk samarbeid på forsvarsmateriellområdet mellom Danmark, Finland, Norge og Sverige”/“Säkerhetsskyddsavtal. Överenskommelse rörande säkerhetsskyddets utformning inom ramen för avtalet om nordisk samarbete inom försvarsmaterielområdet mellan Danmark, Finland, Norge och Sverige“. 1994/1995.

Classified Information exchanged under the above-mentioned Agreements and Arrangements shall continue to be protected in accordance with the terms of this Agreement.

This Agreement is produced in a single copy in the English, Danish, Finnish, Icelandic, Norwegian and Swedish languages. In case of differences of interpretation, the English text shall prevail. The signed copy of this Agreement shall be deposited in the archives of the Ministry of Foreign Affairs of the Kingdom of Norway. The Ministry of Foreign Affairs of the Kingdom of Norway shall transmit certified copies to all the Parties.

Till bekräftelse härav har undertecknade vederbörligen bemyndigade företrädare för respektive regering, undertecknat detta avtal. Upprättat i Oslo, den 7 maj 2010.

In witness whereof the duly authorised representatives of their respective Governments have signed this Agreement. Done in Oslo, this 7 day of May, two thousand and ten

För Konungariket Danmarks regering

On behalf of the Government of the Kingdom of Denmark

För Republiken Finlands regering

On behalf of the Government of the Republic of Finland

För Islands regering

On behalf of the Government of Iceland

För Konungariket Norges regering

On behalf of the Government of the Kingdom of Norway

För Konungariket Sveriges regering

On behalf of the Government of the Kingdom of Sweden