

Regeringens proposition till Riksdagen om godkännande av överenskommelsen mellan Finland och Slovenien om utbyte och ömsesidigt skydd av säkerhetsklassificerad information och med förslag till lag om sättande i kraft av de bestämmelser i överenskommelsen som hör till området för lagstiftningen

PROPOSITIONENS HUVUDSAKLIGA INNEHÅLL

I propositionen föreslås att riksdagen godkänner överenskommelsen mellan Finland och Slovenien om utbyte och ömsesidigt skydd av säkerhetsklassificerad information samt lagen om sättande i kraft av de bestämmelser i överenskommelsen som hör till området för lagstiftningen.

Syftet med överenskommelsen är att säkerställa förmedling och skydd av sekretessbelagd information mellan Finland och Slovenien i utrikes-, försvars-, säkerhets- och polisärenden samt i industri- eller teknologinärenden. Det är fråga om känsligt informa-

tionsmaterial som särskilt har klassificerats på en hög säkerhetsnivå i den utlämnande fördragsslutande staten.

Överenskommelsen träder i kraft den första dagen den andra månaden efter att den senare underrättelsen har tagits emot om att de åtgärder som den nationella lagstiftningen kräver för att sätta överenskommelsen i kraft har slutförts. Lagen om sättande i kraft av överenskommelsen avses träda i kraft samtidigt som överenskommelsen för Finlands del träder i kraft vid en tidpunkt som bestäms genom förordning av republikens president.

INNEHÅLL

PROPOSITIONENS HUVUDSAKLIGA INNEHÅLL	1
INNEHÅLL	2
ALLMÄN MOTIVERING	3
1 INLEDNING	3
2 NULÄGE	4
2.1 Lag om internationella förpliktelser som gäller informationssäkerhet.....	4
<i>Lagens allmänna tillämpningsområde</i>	4
<i>Lagens förhållande till offentlighetslagstiftningen.....</i>	4
<i>Tillämpning av lagen på näringsidkare</i>	4
<i>Verkställande myndigheter.....</i>	5
<i>Sekretessbeläggning och reglering av informationsanvändningen.....</i>	6
<i>Säkerhetsklassificering och -åtgärder.....</i>	6
<i>Personsäkerhet</i>	6
<i>Säkerhetsutredning som gäller sammanslutning.....</i>	7
2.2 Lagstiftning om säkerhetsutredningar	7
3 MÅLSÄTTNING	7
4 PROPOSITIONENS KONSEKVENSER.....	8
4.1 Konsekvenser för medborgarna.....	8
4.2 Konsekvenser för näringslivet.....	8
4.3 Ekonomiska konsekvenser	8
4.4 Konsekvenser för förvaltningen	9
5 BEREDNINGEN AV PROPOSITIONEN.....	9
DETALJMOTIVERING	10
1 Överenskommelsens innehåll och förhållande till lagstiftningen i Finland	10
2 Lagförslag.....	14
3 Ikraftträdande	14
4 Behovet av riksdagens samtycke och behandlingsordning	14
4.1 Behovet av riksdagens samtycke.....	14
4.2 Behandlingsordning.....	16
LAGFÖRSLAG	18
om sättande i kraft av de bestämmelser i överenskommelsen med Slovenien om	
ömsesidigt skydd och utbyte av säkerhetsklassificerad information som hör till	
området för lagstiftningen	18
FÖRDRAGSTEXT	19

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 utplåning.

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 informationssäkerhets-samarbetet, 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 emellertid också en växande betydelse för det ekonomiska, industriella och teknologiska samarbetet, där allt flera projekt på företagsnivå förutsätter tillgång till klassificerad information. Det här gäller särskilt då det är fråga om en myndighetsanskaffning som förutsätter att sekretessbelagd statlig information ges ut till ett företag för att ett kommersiellt 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. Överenskommelsen trädde i kraft den 16 juli 2004 (FördrS 96-97/2004). Ett år senare undertecknades ett avtal mellan Finland och Frankrike och det trädde i kraft den 1 augusti 2005 (FördrS 66-67/2005). Bägge länder 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 94-95/2004). En av de viktigaste målsättningarna med överenskommelsen har varit att säkerställa det finländska näringslivets möjligheter att på jämlik grund med de andra medlemsländerna kunna delta i ESA:s säkerhetsklassificerade anbuds-förfaranden.

Utöver nämnda fördrag har Finland gällande överenskommelser om informationssäkerhet med Slovakien (FördrS 116-117/2007), Estland (FördrS 12-13/2008), Italien (FördrS 23-24/2008), Lettland (FördrS 33-34/2008) och Polen (FördrS 46-47/2008). Under pågående år har Finland utöver det föreliggande avtalet med Slovenien även undertecknat informationssäkerhetsöverenskommelser med Bulgarien (16.4.2008) och Tjeckien (22.5.2008). Avtalen med Spanien, Litauen och Nederländerna har framskridit till paraferingsskedet. Ett projekt är som bäst på gång

också om en överenskommelse för skydd av säkerhetsklassificerad information EU-länderna emellan.

Överenskommelsen mellan Finland och Slovenien undertecknades i Ljubljana den 6 maj 2008. Den har till största delen förhandlats fram utgående från ett modellavtal som Finland lade fram som underlag för förhandlingarna.

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 överenskommelser 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 som har sänts till en finländsk myndighet och avsändaren i enlighet med en internationell överenskommelse som är bindande för Finland eller med någon annan internationell förpliktelse har försett försändelsen med en säkerhetsklassificering. Äganderätten till den överlämnade informationen består även efter överlåtelsen hos den stat som har överlämnat den. 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 till-

ämpningsområde 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 sä-

kerhetsklassificerat 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 anbuds-förfarande 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 anbuds-förfarande 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

Det finns bestämmelser i lag om vilka 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 och skyddspolisen kan verka som utsedda säkerhetsmyndigheter (Designated Security Authority, DSA). Dessa myndigheter ska t.ex. svara för säkerhetsklassificeringen av handlingar i anslutning till anbuds- och upphandlingsförfaranden. Skyddspolisen och huvudstaben svarar för utredningar som gäller personsäkerhet. Säkerhetsutredningar som gäller sammanslutningar görs däremot i sin helhet av huvudstaben.

Det finns bestämmelser i lag om myndigheters och näringsidkares informationsskyldighet. Syftet med bestämmelserna är att säkerställa att behöriga säkerhetsmyndigheter får den information 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. 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.

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

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.

Säkerhetsklassificering och -åtgärder

I lagen föreskrivs om skyldigheten att förse särskilt känsligt informationsmaterial med anteckning om säkerhetsklass. Anteckningen anger vilka åtgärder som ska vidtas vid hantering av materialet. 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 §).

Vid hantering av säkerhetsklassificerat material ska det enligt lagen ses till att materialet förvaras i ändamålsenliga utrymmen. Genom förordning av statsrådet kan det också föreskrivas om säkerhetskrav för dessa utrymmen (10 §).

I lagen om internationella förpliktelser som gäller informationssäkerhet har det i internationella överenskommelser allmänna kravet skrivits in att myndigheterna ska iaktta stor restriktivitet vid användningen av säkerhetsklassificerad information och att endast per-

soner som behöver informationen för skötseln av sina uppgifter ska ges tillgång till den. Dessa personer ska namnges på förhand såvida detta förutsätts i överenskommelsen. Detsamma gäller näringsidkare, så 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). Sålunda fastställs t.ex. den persons 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.). Bestämmelsen är exaktare än lagen om säkerhetsutredningar och i den beaktas vilken typ av internationell förpliktelse det är fråga om.

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 sä-

kerhetsmyndigheten eller, om så har överenskommits mellan säkerhetsmyndigheterna, av den för uppgiften utsedda säkerhetsmyndigheten.

Utgående från bedömningen utfärdas det ett personligt säkerhetsintyg (Personal Security Clearance). Intyget skickas vanligtvis till den fördragsslutande partens säkerhetsmyndighet på det sätt som anges i överenskommelsen. 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. Vid utredningen skall de omständigheter som anges i lagen beaktas, bland annat hur man kan skydda säkerhetsklassificerad information från att obehörigen röjas, ändras eller utplånas eller hur man kan förhindra obehörigt tillträde till utrymmen där säkerhetsklassificerad information hanteras eller där det bedrivs verksamhet som avses i ett säkerhetsklassificerat kontrakt.

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).

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 uppräkningslista 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.

3 Målsättning

Syftet med propositionen är att sätta i kraft överenskommelsen om informationssäkerhet mellan Finland och Slovenien och så förbättra samarbetet mellan länderna samt att trygga

finländska företags möjligheter att delta i internationella eller finsk-slovenska projekt som kan kräva utbyte av känslig sekretessbelagd information.

4 Propositionens konsekvenser

4.1 Konsekvenser för medborgarna

Genom att överenskommelsen sätts i kraft kommer lagen om internationella förpliktelser som gäller informationssäkerhet att tillämpas på säkerhetsklassificerad information och säkerhetsklassificerat material som sänds från Slovenien 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.

Överenskommelsen mellan Finland och Slovenien gäller handlingar som den ena fördragsslutande parten anser att ska vara sekretessbelagda och således har försett med hög säkerhetsklassificering. Denna typ av handlingar är i regel sekretessbelagda också enligt 24 § 1 mom. 2 punkten i offentlighetslagen. Den största skillnaden består i att den myndighet som ska besluta om utlämnandet 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. Myndigheten måste således säkerställa att klassificeringen av en handling svarar mot den som anges i överenskommelsen. 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 överenskommelsen om informationssäkerhet mellan Finland och Slovenien strängt taget inte minskar medborgarnas tillgång till information i jämförelse med tillgången till information i enlighet med den allmänna lagstiftningen.

Personssäkerheten är en viktig del av informationssäkerheten. Eftersom lagen om internationella förpliktelser som gäller informationssäkerhet 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

Överenskommelsen öppnar, i motsats till tidigare, möjligheter för den finländska industrin att få beställningar eller att delta i projekt som förutsätter tillgång till information som är säkerhetsklassificerad i Slovenien. Analogt öppnar överenskommelsen möjligheter för den slovenska industrin att i motsats till tidigare 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.

I det här sammanhanget är det dock skäl att nämna den ändring i lagen om internationella förpliktelser som gäller informationssäkerhet som är under arbete. Med stöd av den skulle skyddspolisen framdeles ansvara för säkerhetsutredningar som gäller civila sammanslutningar, möjligen redan från början av år 2009. För närvarande svarar huvudstaben för alla säkerhetsutredningar som gäller sammanslutningar. De ekonomiska, administrativa och andra eventuella konsekvenser som ändringen medför kommer att behandlas

ingående i samband med regeringspropositionen i fråga.

4.4 Konsekvenser för förvaltningen

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

5 Beredningen av propositionen

Propositionen har beretts som tjänsteuppdrag vid utrikesministeriet. I beredningen av

överenskommelsen och i förhandlingarna har deltagit representanter för utrikesministeriet, justitieministeriet, försvarsministeriet samt arbets- och näringsministeriet.

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

I utlåtandena förordas ett snabbt godkännande och ikraftsättandet av överenskommelsen. Vid den fortsatta beredningen har synpunkterna i utlåtandena beaktats.

DETALJMOTIVERING

1 Överenskommelsens innehåll och förhållande till lagstiftningen i Finland

Artikel 1. Definitioner. I artikel 1 definieras de begrepp som är centrala i tillämpningen av överenskommelsen.

Med säkerhetsklassificerad information avses information, handling eller material som de fördragsslutande parterna förmedlar eller framställer sinsemellan, som har säkerhetsklassificerats i enlighet med nationell lagstiftning och försetts med korrekt säkerhetsklassbeteckning. Säkerhetsklassificerad information ska skyddas mot olovligt röjande, missbruk eller försvinnande.

Med säkerhetsklassificerat kontrakt avses kontrakt eller underleverantörskontrakt, inbegripet förhandlingar som föregår kontrakt, där det ingår eller som kräver tillgång till säkerhetsklassificerad information. Det här är i samklang med 3 punkten i 2 § i lagen om internationella förpliktelser som gäller informationssäkerhet.

Med utlämnande part avses fördragsslutande part, inbegripet offentlig- och privaträttsliga juridiska personer inom dess jurisdiktion, som lämnar ut säkerhetsklassificerad information till mottagarparten. Det handlar alltså om ägaren till den säkerhetsklassificerade informationen.

Med mottagarpart avses fördragsslutande part, inbegripet offentlig- och privaträttsliga juridiska personer inom dess jurisdiktion, som mottar säkerhetsklassificerad information av den utlämnande parten.

Med tredje part avses en stat, inbegripet offentlig- och privaträttsliga juridiska personer inom dess jurisdiktion, eller internationell organisation, som inte är part i detta fördrag.

Med informationsbehov avses principen, enligt vilken information endast får överlätas till en person som har behov av tillgång till säkerhetsklassificerad information i samband med officiella uppgifter eller för ett konkret uppdrag. Definitionen motsvarar bestämmelserna i 6 § 3 mom. i lagen om internationella förpliktelser som gäller informationssäkerhet.

Artikel 2. Syfte och tillämpningsområde. I artikeln definieras det att syftet med överenskommelsen är att skydda säkerhetsklassificerad information som Finland och Slovenien förmedlar till varandra. Här definieras också de områden överenskommelsen ska tillämpas på. De är utrikes-, försvars-, säkerhets- och polisärenden samt industri- eller teknologiärenden. Upprätthållandet av gränssäkerheten anses ingå i dessa ärenden. Överenskommelsen ska alltså endast tillämpas på förmedling av information som rör dessa områden eller som framställs eller förmedlas i dessa sammanhang.

Överenskommelsen tillämpas inte endast på myndighetsrelationer utan också på kontrakt, i första hand av ekonomisk karaktär, där ena parten är ett privat företag eller en privat sammanslutning och som, anbudsskedet inbegripet, förutsätter tillgång till information eller material som har säkerhetsklassificerats.

Artikel 3. Behöriga säkerhetsmyndigheter. I stycke 1 fastställs de behöriga säkerhetsmyndigheterna i vardera fördragsstaten. Nationell säkerhetsmyndighet i Finland (National Security Authority, NSA) är enligt lagen om internationella förpliktelser som gäller informationssäkerhet utrikesministeriet, där uppgiften handhas av säkerhetsenheten. I Slovenien handhas uppgiften av Urad Vlade Republike Slovenije za varovanje tajnih podatkov. I stycke 2 åläggs säkerhetsmyndigheterna att underrätta varandra om övriga behöriga myndigheter som har ansvar för genomförandet av överenskommelsen. I Finland är de särskilt utsedda säkerhetsmyndigheterna enligt 4 § i lagen om internationella förpliktelser som gäller informationssäkerhet huvudstaben, skyddspolisen och försvarsministeriet. Enligt stycke 3 är de fördragsslutande parterna skyldiga att underrätta varandra om eventuella ändringar som gäller de nationella säkerhetsmyndigheterna.

Artikel 4. Säkerhetsklasserna. I artikeln definieras hur Finlands och Sloveniens säkerhetsklasser motsvarar varandra. Bägge stater har fyra säkerhetsklasser. Även den

engelska översättningen på respektive klass anges.

Den högsta säkerhetsklassen, som kräver de strängaste informationssäkerhetsåtgärderna, är YTTERST HEMLIG (STROGO TAJNO). 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 punkt 10 och säkerheten i punkterna 5, 8 och 9 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 HEM-LIG (TAJNO). 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 KONFIDENTIELL (ZAUPNO), varmed i Finland avses information som, om den obehörigen röjs, kan skada försvaret, säkerheten, de internationella relationerna eller andra allmänna intressen.

Till den fjärde klassen av dokument, BEGRÄNSAD TILLGÅNG (INTERNO), hör information som, om den obehörigen röjs, kan skada allmänna intressen eller försämra myndigheternas möjligheter att agera.

Artikel 5. Tillgång till säkerhetsklassificerad information.

Artikeln handlar om personsäkerhet. Enligt stycke 1 kan tillgång till information i den lägsta säkerhetsklassen BEGRÄNSAD TILLGÅNG beviljas personer som har ett informationsbehov och som har informerats om ansvaret och skyldigheterna det är för-enat med. Enligt stycke 2 krävs det för tillgång till information i säkerhetsklassen KONFIDENTIELL och högre därutöver att personen har säkerhetsklarerats i enlighet med nationell lagstiftning. Bestämmelsen är i överensstämmelse med 6 § 3 mom. i lagen om internationella förpliktelser som gäller

informationssäkerhet, där endast personer som behöver informationen för skötseln av sina uppgifter ges tillgång till informationsmaterialet. Den kontroll av en persons tillförlitlighet som internationella informationssäkerhetsförpliktelser kräver utförs i Finland i enlighet med lagen om säkerhetsutredningar och med 11 § i lagen om internationella förpliktelser som gäller informationssäkerhet. Personsäkerhetsutredningarna görs av huvudstaben i ärenden som gäller försvarsförvaltningen, i övriga fall av skyddspolis.

Enligt stycke 3 förbinder sig de fördrags-slutande parterna att erkänna varandras säkerhetsklarerings.

Artikel 6. Skydd av säkerhetsklassificerad information. Stycke 1 innehåller den viktigaste principen i överenskommelsen, enligt vilken de fördragsslutande parterna åtar sig att skydda säkerhetsklassificerad information på samma nivå som egen information i motsvarande nationella säkerhetsklass.

I stycke 2 räknas de skyldigheter upp som den utlämnande partens behöriga säkerhetsmyndighet har för att skydda säkerhetsklassificerad information. Enligt a-punkten ska myndigheten säkerställa att den säkerhetsklassificerade informationen märks med korrekt säkerhetsbeteckning i enlighet med nationell lagstiftning. Enligt b-punkten ska den behöriga säkerhetsmyndigheten underrätta mottagarparten om eventuella överlåtelsevillkor eller restriktioner i användningen av informationen och om eventuella senare ändringar i klassificeringen.

Stycke 3 innehåller analogt de skyldigheter mottagarpartens behöriga säkerhetsmyndighet har för att skydda säkerhetsklassificerad information. Enligt a-punkten ska myndigheten säkerställa att mottagen säkerhetsklassificerad information märks med motsvarande säkerhetsbeteckning. Enligt b-punkten ska myndigheten också säkerställa att säkerhetsklassen inte ändras utan skriftligt tillstånd av den utlämnande parten.

Artikel 7. Restriktioner i användningen av säkerhetsklassificerad information. Artikeln innehåller de viktigaste utfästelserna rörande ömsesidigt skydd av information.

Enligt stycke 1 får säkerhetsklassificerad information inte användas för något annat

ändamål än det den har utlämnats för och med de restriktioner den utlämnande parten har föreskrivit. Förpliktelsen motsvaras av bestämmelsen i 6 § 2 mom. i lagen om internationella förpliktelser som gäller informationssäkerhet.

Stycke 2 innehåller ett förbud mot att lämna ut säkerhetsklassificerad information till tredje part utan skriftligt samtycke på förhand av den utlämnande partens behöriga säkerhetsmyndighet. I 6 § 1 mom. i lagen om internationella förpliktelser som gäller informationssäkerhet finns det en specialbestämmelse om sekretessbeläggning, enligt vilken information som har säkerhetsklassificerats i enlighet med en internationell överenskommelse om informationssäkerhet ska vara sekretessbelagd.

Artikel 8. Förmedling av säkerhetsklassificerad information.

Artikeln innehåller bestämmelser om tillvägagångssättet vid överföring av säkerhetsklassificerad information mellan de fördragsslutande parterna. Enligt artikeln ska informationen förmedlas via diplomatiska eller militära kanaler, eller andra kanaler som har godkänts av de behöriga säkerhetsmyndigheterna. Information i säkerhetsklassen BEGRÄNSAD TILLGÅNG får också förmedlas per post eller med någon annan förmedlingstjänst i enlighet med nationell lagstiftning. Bestämmelser om hanteringskraven för de olika säkerhetsklasserna finns i 9 § i lagen om internationella förpliktelser som gäller säkerhetsklassificerad information. Bestämmelser om säkerhetsåtgärderna i de olika säkerhetsklasserna som ska beaktas i hanteringen av särskilt känsligt informationsmaterial kan utfärdas genom förordning av statsrådet.

Artikel 9. Kopiering, översättning och utplåning av säkerhetsklassificerad information.

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

Stycke 1 innehåller en förpliktelse att förse alla kopior och översättningar av säkerhetsklassificerad information med korrekt säkerhetsbeteckning. Översättningarna och antalet kopior ska begränsas till minsta möjliga som är nödvändigt för officiella ändamål. Över-

sättningar ska enligt stycke 2 förses med en korrekt anmärkning på översättningsspråket om att texten innehåller säkerhetsklassificerad information.

Stycke 3 innehåller ett förbud att översätta eller kopiera information i säkerhetsklassen YTTERST HEMLIG utan skriftligt förhandstillsånd av säkerhetsmyndigheten hos den part som har lämnat ut materialet. Nationella bestämmelser om hur förpliktelsen ska uppfyllas kan vid behov utfärdas med stöd av 9 § i lagen om internationella förpliktelser som gäller informationssäkerhet.

Enligt stycke 4 får information i klassen YTTERST HEMLIG inte utplånas, utan ska returneras till den utlämnande parten när de fördragsslutande parterna anser att den inte längre behövs. 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 HEMLIG eller lägre ska enligt stycke 5 utplånas i enlighet med nationell lagstiftning när mottagarparten anser att den inte längre behövs.

Artikel 10. Säkerhetsklassificerade kontrakt.

Artikeln innehåller bestämmelser om situationer där endera fördragsslutande parten ingår eller ger en kontraktspart inom sin jurisdiktion tillstånd att ingå ett säkerhetsklassificerat kontrakt med en kontraktspart som lyder under den andra fördragsslutande partens jurisdiktion.

Enligt stycke 1 ska den utlämnande partens behöriga säkerhetsmyndighet av mottagarpartens behöriga säkerhetsmyndighet på begäran bli underrättad om huruvida en kontraktspart har utfärdats ett nationellt säkerhetsintyg i den säkerhetsklass som krävs. Syftet med bestämmelsen är att trygga den utlämnande partens fria provningsrätt i beredningen av kontrakt.

Enligt stycke 2 kan mottagarpartens behöriga säkerhetsmyndighet likväl vid öppna anbudsförfaranden, som inte är riktade till något särskilt land eller företag, utan formell begäran tillställa den utlämnande partens behöriga säkerhetsmyndighet de säkerhetsintyg som avses i stycke 1. Syftet med bestämmelsen är att försnabba finländska företags eller reciprok slovenska företags tillträde till sä-

kerhetsklassificerad information som krävs för att ställa en offert, vilket i sin tur är ägnat att effektivisera företagets offertberedning och förbättra deras konkurrensställning.

I stycke 3 jämföras underleverantörer med kontraktspartier när det gäller kraven på informationssäkerhet som nämns i stycke 1 och 2.

Stycke 4 möjliggör att mottagarparten företar säkerhetsinspektioner i sina anläggningar på förslag av den utlämnande parten. Avsikten med inspektionerna är att säkerställa att anläggningarna uppfyller överenskommelsens bestämmelser. Den utlämnande partens säkerhetsmyndighet har rätt att delta i dessa inspektioner.

Nationella bestämmelser om säkerhetsklassificerade kontrakt finns i 1 § 2 mom. (tillämpning på näringsidkare), i 2 § 2 punkten (särskilt känsligt informationsmaterial), i 7 § (tystnadsplikt och förbud mot utnyttjande) samt i 12 (säkerhetsutredningar som gäller sammanslutningar) och 13 § i lagen om internationella förpliktelser som gäller informationssäkerhet. I lagens 13 § finns det bestämmelser om förbindelser som en kontraktspart kan ingå om att vidta säkerhetsåtgärder. De nationella bestämmelserna motsvarar förpliktelserna i överenskommelsen. Finska myndigheters rätt att lämna ut information, som är nödvändig för att uppfylla förpliktelsen, finns föreskriven i 17 § i lagen om internationella förpliktelser som gäller informationssäkerhet.

Artikel 11. Besök. Artikeln innehåller bestämmelser om de förfaranden som ska följas när det anordnas tillfällen för en fördragsslutande parts representanter att bekanta sig med den andra fördragsslutande partens lokaler, där säkerhetsklassificerad information utvecklas, hanteras, framställs eller förvaras, eller där det genomförs säkerhetsklassificerad projekt.

Enligt stycke 1 krävs besök i lokaler, där säkerhetsklassificerad information hanteras, förhandstillstånd av värdlandets behöriga säkerhetsmyndighet. I stycke 2 föreskrivs det att begäran om besök ska företas värdlandets behöriga säkerhetsmyndighet minst 20 dagar före besöket. I stycke 2 ingår också närmare bestämmelser om vilka uppgifter som ska ingå i en begäran.

I stycke 3 konstateras det att de behöriga säkerhetsmyndigheterna i brådskande fall kan avtala om en kortare tidsfrist för att företa en begäran.

Enligt stycke 4 kan de behöriga säkerhetsmyndigheterna göra upp förteckningar över besökare med tillstånd till upprepade besök. Förteckningen ska gälla i högst 12 månader, därefter kan giltighetstiden förlängas med högst 12 månader. När en förteckning har godkänts kan respektive organisationer arrangera sina besök direkt sinsemellan. Enligt stycke 5 ska säkerhetsklassificerad information som en besökare förvärvar anses som säkerhetsklassificerad information under denna överenskommelse.

Bestämmelser om besök finns i 18 § i lagen om internationella förpliktelser som gäller informationssäkerhet.

Artikel 12. Säkerhetssamarbete.

Artikeln innehåller bestämmelser om samarbetet mellan de fördragsslutande parternas myndigheter för att säkerställa genomförandet av överenskommelsen.

Enligt stycke 1 ska de fördragsslutande parternas behöriga säkerhetsmyndigheter underrätta varandra om sina nationella säkerhetsnormer och -förfaranden och sin praxis för skydd av säkerhetsklassificerad information. De behöriga säkerhetsmyndigheterna kan också besöka varandra för att bekanta sig med dessa system. Syftet med besöken är att ta reda på hurdana förfaranden för skydd av säkerhetsklassificerad information den andra fördragsslutande parten har.

I stycke 2 krävs det att de behöriga säkerhetsmyndigheterna ska underrätta varandra om exceptionella säkerhetsrisker som kan äventyra sekretessen hos säkerhetsklassificerad information. På begäran ska de behöriga säkerhetsmyndigheterna enligt stycke 3 i enlighet med nationell lagstiftning bistå varandra i förfaranden i anslutning till säkerhetsutredningar. Stycke 4 ålägger säkerhetsmyndigheterna att utan dröjsmål underrätta varandra om ändringar som gäller säkerhetsintyg. I stycke 5 ges de fördragsslutande parternas säkerhetsmyndigheter tillstånd att direkt sinsemellan utbyta operativa eller underrättelseuppgifter i enlighet med nationell lagstiftning. Enligt stycke 6 ska samarbetet som sker

med stöd av överenskommelsen föregå på engelska.

Artikel 13. Sekretessbrott. Enligt stycke 1 är en fördragsslutande parts säkerhetsmyndighet skyldig att utan dröjsmål underrätta den andra fördragsslutande partens säkerhetsmyndighet om misstänkta eller upptäckta fall av sekretessbrott. Den fördragsslutande part, till vars jurisdiktion ärendet hör, ska enligt stycke 2 i enlighet med sin nationella lagstiftning vidta alla åtgärder som är möjliga för att begränsa följderna av sekretessbrottet och för att förhindra fortsatta kränkningar. Den andra fördragsslutande parten ska vid behov bistå undersökningen. I varje fall ska den andra parten få besked om undersökningens resultat och om åtgärder som har vidtagits på grund av kränkningen. Bestämmelserna som krävs för att genomföra de förpliktelser som avses i artikeln ingår i 19 § i lagen om internationella förpliktelser som gäller informationssäkerhet.

Artikel 14. Kostnader. Enligt artikeln ska vardera fördragsslutande parten själv stå för de kostnader som förorsakas dem i samband med genomförandet av överenskommelsen.

Artikel 15. Tolkning och lösning av tvister.

Enligt artikeln ska tvister som uppkommer angående tolkning eller tillämpning av överenskommelsen uteslutande avgöras i samråd mellan parterna.

Artikel 16. Slutbestämmelser. Artikeln innehåller bestämmelser om ikraftträdandet av överenskommelsen, ändringar i den samt om uppsägning av den. Överenskommelsen har ingåtts tills vidare och den kan ändras på gemensam överenskommelse mellan de fördragsslutande parterna. En uppsägning träder i kraft sex månader efter att meddelandet om uppsägning har tagits emot. Oberoende av en uppsägning ska all säkerhetsklassificerad information som har lämnats ut under överenskommelsen fortsättningsvis skyddas i enlighet med dess bestämmelser, tills den utlämnande parten befriar mottagarparten från denna skyldighet.

2 Lagförslag

I 95 § i grundlagen förutsätts att bestämmelser i internationella förpliktelser som hör till området för lagstiftningen sätts i kraft natio-

nellt 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 säkerhetsöverenskommelsen mellan Finland och Slovenien, innehåller propositionen endast ett förslag till en blankettlag.

1 §. Genom bestämmelsen i lagförslaget 1 § sätts de bestämmelser i överenskommelsen i kraft som hör till området för lagstiftningen. De bestämmelser som hör till området för lagstiftningen refereras nedan i avsnittet om riksdagens samtycke.

2 §. Om lagens ikraftträdande bestäms genom förordning av republikens president. Avsikten är att lagen sätts i kraft samtidigt som överenskommelsen träder i kraft för Finlands del.

3 Ikraftträdande

Enligt artikel 16.1 i överenskommelsen mellan Finland och Slovenien ska de fördragsslutande parterna underrätta varandra när de åtgärder har slutförts som den nationella lagstiftningen kräver för att sätta överenskommelsen i kraft. Överenskommelsen träder i kraft den första dagen den andra månaden efter att den senare underrättelsen har tagits emot.

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

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 den överenskommelse som ingår i propositionen riksdagens samtycke. I *artikel 1* definieras vad som avses med säkerhetsklassificerad information och säkerhetsklassificerade kontrakt. I *artikel 2* definieras sedan överenskommelsens syfte och tillämpningsområde. Eftersom dessa bestämmelser i överenskommelsen 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* ställs det fast att utrikesministeriet är Finlands nationella säkerhetsmyndighet. Bestämmelsen motsvarar 4 § 1 mom. i lagen om internationella förpliktelser som gäller informationssäkerhet. Bestämmelsen är konstaterande och ska därför inte anses förutsätta riksdagens samtycke.

Restriktioner i användningen av säkerhetsklassificerad information och restriktioner som gäller personer med tillgång till säkerhetsklassificerad information kommer till uttryck i *artikel 5*. Här finns föreskrifter om de fördragsslutande parternas skyldighet att göra relevanta säkerhetsutredningar över personer som har eller kan ha tillträde till sådan säkerhetsklassificerad information som avses i överenskommelsen. I upplägget för säkerhetsutredningar ska det som sägs i 10 § 1 mom. i grundlagen om tryggt privatliv och om plikten att lagstifta om skydd för personuppgifter beaktas. I Finland finns det föreskrifter om personer som är föremål för sä-

kerhetsutredningar samt om utredningsförfarandet i lagen om säkerhetsutredningar.

I *artiklarna 6 och 7* finns det föreskrifter om de nationella åtgärder som krävs för att skydda säkerhetsklassificerad information inom överenskommelsens tillämpningsområde och som begränsar förmedlingen och användningen av samt tillträdet till denna information. De fördragsslutande parterna är enligt artikel 6 ålagda att skydda denna säkerhetsklassificerade information på samma nivå som de skyddar egen information i motsvarande säkerhetsklass, vilket innebär att mottagen säkerhetsklassificerad information ska märkas korrekt. Mottagarparten ska enligt huvudregeln i artikel 7 hålla den säkerhetsklassificerade informationen hemlig.

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 lagens 25 § ska det göras en sekretessanteckning i handlingar som en myndighet ger ut till sakägare 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 sekretessbeläggas. I 8 § i samma lag finns det också 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 försees 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 överenskommelsen ställer följaktligen strängare krav än den finländska lagstiftningen på anteckning om sekretess i säkerhetsklassificerad information. Bestämmelserna kräver riksdagens samtycke.

I *artikel 8* finns det bestämmelser om förmedlingen av säkerhetsklassificerad information och i *artikel 9* om översättning, kopiering och utplåning av säkerhetsklassificerad information. Bestämmelser om hanteringskraven för de olika säkerhetsklasserna finns i 9 § i lagen om internationella förpliktelser som gäller säkerhetsklassificerad information. Bestämmelser om säkerhetsåtgärderna i de olika säkerhetsklasserna som ska följas vid hanteringen av särskilt känsligt informationsmaterial kan utfärdas genom förordning av statsrådet.

I *artikel 10* finns det bestämmelser om säkerhetsklassificerade kontrakt och om de säkerhetsutredningar som sådana kontrakt kräver. Föreskrifter om säkerhetsutredningar som gäller sammanslutningar ingår i 12 och 13 § i lagen om internationella förpliktelser om informationssäkerhet.

I *artikel 11* finns det bestämmelser om besök av fysiska personer från den ena fördragsslutande parten till den andra fördragsslutande partens, alltså värdpartens lokaler, där det hanteras säkerhetsklassificerad information. Syftet med besök av de fördragsslutande parternas representanter är att säkerställa att överenskommelsens syfte om ett korrekt skydd för säkerhetsklassificerad information förverkligas. Denna besöksrätt innehåller inget sådant utövande av offentlig makt eller sådan granskningsrätt som står i konflikt med grundlagen (GrUU 179/1997). Genom bestämmelsen i överenskommelsen uppkommer det indirekt en skyldighet även 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 överenskommelsens besöksbestämmelse.

I *artikel 13* krävs det att den fördragsslutande partens behöriga säkerhetsmyndighet omedelbart underrättar den andra partens behöriga säkerhetsmyndighet ifall sekretessen i säkerhetsklassificerad information har brutits eller det finns en misstanke om att så har skett. De fördragsslutande parterna måste utreda överträdelser av sekretessbestämmelserna för säkerhetsklassificerad information och så långt det är möjligt vidta åtgärder ock-

så då ett sekretessbrott sker i tredje land. I 19 § i lagen om internationella förpliktelser som gäller informationssäkerhet föreskrivs om de nationella säkerhetsmyndigheternas skyldigheter i sådana situationer som avses i överenskommelsens bestämmelser.

4.2 Behandlingsordning

Bestämmelser som är av betydelse för behandlingsordningen ingår i överenskommelsens artiklar 5–7, där det ställs begränsningar för offentligheten när det gäller information och material som har säkerhetsklassificerats. Fördragsbestämmelserna 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 i internationella samt finsk-slovenska bilaterala aktiviteter och projekt som kräver utbyte av känslig och sekretessbelagd information kan anses vara ett sådant tvingande skäl. En specialbestämmelse om sekretess ingår i 6 § i lagen om internationella förpliktelser som gäller informationssäkerhet.

Den mellan Finland och Slovenien ingångna överenskommelsen om ömsesidigt skydd och utbyte av säkerhetsklassificerad information 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 överenskommelsen följaktligen godkännas med enkel majoritet och förslaget om sättande i kraft av de bestämmelser i överenskommelsen som hör till området för lagstiftningen godkännas i vanlig lagstiftningsordning.

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

att Riksdagen godkänner den i Ljubljana den 6 maj 2008 mellan Republiken Finland och Republiken Slovenien ingångna överenskommelsen om ömsesidigt skydd och utbyte av säkerhetsklassificerad information.

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

Lagförslag

Lag

om sättande i kraft av de bestämmelser i överenskommelsen med Slovenien om ömsesidigt skydd och utbyte av säkerhetsklassificerad information som hör till området för lagstiftningen

I enlighet med riksdagens beslut föreskrivs:

1 §
De bestämmelser som hör till området för lagstiftningen i den i Ljubljana den 6 maj 2008 mellan Republiken Finland och Republiken Slovenien ingångna överenskommelsen om ömsesidigt skydd och utbyte av sä-

kerhetsklassificerad information gäller som lag sådana Finland har förbundit sig till dem.

2 §
Om ikraftträdandet av denna lag bestäms genom förordning av republikens president.

Helsingfors den 3 oktober 2008

Republikens President

TARJA HALONEN

Utrikesminister *Alexander Stubb*

(Översättning)

Fördragstext

Överenskommelse**Agreement****mellan Republiken Finlands regering
och****between
the Government of the Republic of
Finland****Republiken Sloveniens regering
om****and
the Government of the Republic of
Slovenia****utbyte och ömsesidigt skydd av säker-
hetsklassificerad information****on
the Exchange and Mutual Protection
of Classified Information**

Republiken Finlands regering och Republiken Sloveniens regering, härafter "de fördragsslutande parterna", som med hänsyn till nationella intressen och av säkerhetsskäl önskar säkerställa skyddet av säkerhetsklassificerad information som de fördragsslutande parterna, eller offentlig- och privaträttsliga juridiska personer inom deras jurisdiktion, utbyter sinsemellan,

The Government of the Republic of Finland and the Government of the Republic of Slovenia, hereinafter referred to as the "Parties", wishing to ensure the protection of Classified Information exchanged between the Parties or between public and private entities under their jurisdiction, in respect of national interests and security,

har kommit överens om följande:

have agreed on the following:

Artikel 1**Article 1***Definitioner**Definitions*

I denna överenskommelse avses följande med dessa begrepp:

For the purposes of this Agreement these terms mean the following:

Säkerhetsklassificerad information: varje slag av information, handling eller material, oavsett form, som de fördragsslutande parterna förmedlar eller framställer sinsemellan i enlighet med endera fördragsslutande partens nationella lagstiftning, som kräver skydd mot olovligt röjande, missbruk eller försvinnande och som har betecknats som sådant och märkts på korrekt sätt.

Classified Information: Any information, document or material, regardless of its form, which is transmitted or generated between the Parties under the national legislation of either Party, requires protection against unauthorised disclosure, misappropriation or loss and is designated as such and marked appropriately.

Säkerhetsklassificerat kontrakt: kontrakt eller underleverantörskontrakt, inbegripet förhandlingar som föregår kontrakt, där det ingår eller som kräver tillgång till säkerhetsklassificerad information.

Classified Contract: A contract or a sub-contract, including pre-contractual negotiations, which contains Classified Information or involves access to it.

Utlämnande part: fördragsslutande part, inbegripet offentlig- och privaträttsliga juridiska personer inom dess jurisdiktion, som ger ut säkerhetsklassificerad information till motparten.

Originating Party: The Party, including any public or private entities under its jurisdiction, which releases Classified Information to the Recipient Party.

Mottagarpart: fördragsslutande part, inbegripet offentlig- och privaträttsliga juridiska

Recipient Party: The Party, including any public or private entities under its jurisdic-

personer inom dess jurisdiktion, som mottar säkerhetsklassificerad information av den utlämnande parten.

Tredje part: stat, inbegripet offentlig- och privaträttsliga juridiska personer inom dess jurisdiktion, eller internationell organisation, som inte är part i detta fördrag.

Informationsbehov: princip, enligt vilken en fysisk person kan ges tillgång till säkerhetsklassificerad information endast i samband med officiella förpliktelser eller uppdrag.

tion, which receives Classified Information from the Originating Party.

Third Party: A state, including any public or private entities under its jurisdiction, or an international organisation that is not a Party to this Agreement.

Need-to-Know: A principle by which access to Classified Information may be granted to an individual only in connection with his/her official duties or tasks.

Artikel 2

Syfte och tillämpningsområde

Syftet med denna överenskommelse är att skydda säkerhetsklassificerad information som de fördragsslutande parterna lämnar till varandra huvudsakligen i samband med utrikes-, försvars-, säkerhets-, och polisärenden, såväl som i industri- eller teknologiärenden, eller som förmedlas i samband med genomförande eller beredning av säkerhetsklassificerade kontrakt eller som uppstår eller produceras i samband med verksamhet i anslutning till överenskommelsens tillämpningsområde.

Article 2

Purpose and Scope of Application

The purpose of this Agreement is to protect Classified Information provided by one Party to the other Party mainly for purposes of foreign affairs, defence, security and police matters as well as industrial or technological matters, or transmitted within the context of the implementation or preparation of Classified Contracts, or arising or produced within the context of an activity falling within the scope of application of this Agreement.

Artikel 3

Behöriga säkerhetsmyndigheter

1. De fördragsslutande parterna har utsett följande nationella säkerhetsmyndigheter att ha det allmänna ansvaret för verkställandet och för korrekt tillsyn av alla aspekter i denna överenskommelse:

I Republiken Finland:
Utrikesministeriet, säkerhetsenheten

I Republiken Slovenien:
Urad Vlade Republike Slovenije za varovanje tajnih podatkov

2. De nationella säkerhetsmyndigheterna ska underrätta varandra om övriga behöriga myndigheter som har ansvar för verkställandet av denna överenskommelse.

3. De fördragsslutande parterna ska underrätta varandra om eventuella senare ändringar som gäller de nationella säkerhetsmyndigheterna.

Article 3

Competent Security Authorities

1. The National Security Authorities designated by the Parties as responsible for the general implementation and the relevant controls of all aspects of this Agreement are:

In the Republic of Finland:
Ulkoasiainministeriö, turvallisuusyksikkö

In the Republic of Slovenia:
Urad Vlade Republike Slovenije za varovanje tajnih podatkov

2. The National Security Authorities shall notify each other of any other Competent Security Authorities that are responsible for the implementation of this Agreement.

3. The Parties shall inform each other of any subsequent changes of the National Security Authorities.

Artikel 4

Säkerhetsklasserna

1. Säkerhetsklassificerad information som lämnas ut i enlighet med denna överenskommelse ska märkas med korrekt säkerhetsklass i enlighet med de fördragsslutande parternas nationella lagstiftning.

2. De nationella beteckningarna för olika säkerhetsklasser motsvarar varandra enligt följande:

Article 4

Security Classifications

1. Classified Information released under this Agreement shall be marked with the appropriate security classification level under the national legislation of the Parties.

2. The equivalence of the national security classification markings is as follows:

Republiken Finland	Slovenian tasavalta	Englanninkielinen käännös
ERITTAIN SALAINEN (YTTERST HEMLIG)	STROGO TAJNO	TOP SECRET
SALAINEN (HEMLIG)	TAJNO	SECRET
LUOTTAMUKSELLINEN (KONFIDENTIELL)	ZAUPNO	CONFIDENTIAL
KÄYTTÖ RAJOITETTU (BEGRÄNSAD TILLGÅNG)	INTERNO	RESTRICTED

Artikel 5

Tillgång till säkerhetsklassificerad information

1. Tillgång till information i säkerhetsklass KÄYTTÖ RAJOITETTU/INTERNO (BEGRÄNSAD TILLGÅNG) får endast beviljas personer som har ett informationsbehov och som har informerats om sitt ansvar och sina skyldigheter.

2. Tillgång till information i säkerhetsklass LUOTTAMUKSELLINEN/ZAUPNO (KONFIDENTIELL) och högre får endast beviljas personer som har ett informationsbehov, som har säkerhetsklarerats i enlighet med nationell lagstiftning och som har tillstånd att få tillgång till sådan information samt informerats om sitt ansvar och sina skyldigheter.

3. De fördragsslutande parterna erkänner ömsesidigt varandras säkerhetsklarerings. Artikel 4.2 ska tillämpas i enlighet med detta.

Article 5

Access to Classified Information

1. Access to information classified as KÄYTTÖ RAJOITETTU/INTERNO shall be limited to persons who have a Need-to-Know and who have been briefed accordingly.

2. Access to information classified as LUOTTAMUKSELLINEN/ZAUPNO and above shall be limited to persons who have a Need-to-Know and who, in accordance with national legislation, have been security cleared and authorized to have access to such information as well as briefed accordingly.

3. The Parties shall mutually recognise their respective security clearances. Paragraph 2 of Article 4 shall apply accordingly.

Artikel 6

Skyddet av säkerhetsklassificerad information

1. De fördragsslutande parterna ska skydda den säkerhetsklassificerade information som avses i denna överenskommelse på samma nivå som egen information i motsvarande säkerhetsklass.

2. Den utlämnande partens behöriga säkerhetsmyndighet ska

a) säkerställa att den säkerhetsklassificerade informationen märks med korrekt säkerhetsbeteckning i enlighet med nationell lagstiftning, och

b) underrätta mottagarparten

- om eventuella överlåtelsevillkor eller restriktioner i användningen av informationen och

- om eventuella senare ändringar i klassificeringen.

3. Mottagarpartens behöriga säkerhetsmyndighet ska

a) säkerställa att den säkerhetsklassificerade informationen märks med motsvarande säkerhetsbeteckning i enlighet med artikel 4.2, och

b) säkerställa att säkerhetsklassen inte ändras utan skriftligt tillstånd av den utlämnande parten.

Artikel 7

Restriktioner i användningen av säkerhetsklassificerad information

1. Mottagarparten får använda den säkerhetsklassificerade informationen endast för det ändamål den har utlämnats för och med de restriktioner den utlämnande parten har föreskrivit.

2. Mottagarparten får inte lämna ut säkerhetsklassificerad information till en tredje part utan den utlämnande partens skriftliga samtycke.

Artikel 8

Förmedling av säkerhetsklassificerad information

1. De fördragsslutande parterna ska förmedla varandra säkerhetsklassificerad information

Article 6

Protection of Classified Information

1. The Parties shall afford to Classified Information referred to in this Agreement the same protection as to their own information of the corresponding level of security classification.

2. The Competent Security Authority of the Originating Party shall:

a) ensure that the Classified Information is marked with an appropriate security classification marking in accordance with its national legislation, and

b) inform the Recipient Party

- of any conditions of release or limitations on the use of the Classified Information, and

- of any subsequent changes in the classification.

3. The Competent Security Authority of the Recipient Party shall:

a) ensure that the Classified Information is marked with an equivalent classification marking in accordance with Paragraph 2 of Article 4, and

b) ensure that the classification level is not changed unless authorized in writing by the Originating Party.

Article 7

Restriction of use of Classified Information

1. The Recipient Party shall use the Classified Information only for the purpose for which it has been delivered and within the limitations stated by the Originating Party.

2. The Recipient Party shall not release Classified Information to a Third Party without a written consent of the Originating Party.

Article 8

Transmission of Classified Information

1. Classified Information shall be transmitted between the Parties through diplomatic or

via diplomatiska eller militära kanaler, eller andra kanaler som har godkänts av de behöriga säkerhetsmyndigheterna i enlighet med nationell lagstiftning.

2. Information i säkerhetsklass KÄYTTÖ RAJOITETTU/INTERNO (BEGRÄNSAD TILLGÅNG) får också förmedlas per post eller med någon annan förmedlingstjänst i enlighet med nationell lagstiftning.

military channels or through other channels approved by their Competent Security Authorities in accordance with national legislation.

2. Information classified as KÄYTTÖ RAJOITETTU/INTERNO may be transmitted also by post or another delivery service in accordance with national legislation.

Artikel 9

Kopiering, översättning och utplåning av säkerhetsklassificerad information

1. Alla kopior och översättningar av säkerhetsklassificerad information ska föras med korrekt säkerhetsbeteckning och skyddas på samma sätt som den säkerhetsklassificerade originalinformationen. Översättningarna och antalet kopior ska begränsas till minsta möjliga som officiella ändamål kräver.

2. Alla översättningar ska föras med en korrekt anteckning på översättningsspråket om att texten innehåller säkerhetsklassificerad information från den utlämnande parten.

3. Säkerhetsklassificerad information med beteckningen ERITTÄIN SALAINEN/STROGO TAJNO (YTTERST HEMLIG) får översättas och kopieras endast med den utlämnande partens skriftliga tillstånd.

4. Säkerhetsklassificerad information med beteckningen ERITTÄIN SALAINEN/STROGO TAJNO (YTTERST HEMLIG) får inte utplånas. Den ska returneras till den utlämnande parten när de fördragsslutande parterna anser att den inte längre behövs.

5. Information i säkerhetsklass SALAINEN/TAJNO (HEMLIG) eller lägre ska utplånas i enlighet med nationell lagstiftning när mottagarparten anser att den inte längre behövs.

Artikel 10

Säkerhetsklassificerade kontrakt

1. Om den utlämnande partens behöriga säkerhetsmyndighet har för avsikt att tillåta förhandlingar om ett säkerhetsklassificerat kontrakt med en kontraktspart inom mottagarpartens jurisdiktion, ska myndigheten på begäran

Article 9

Reproduction, Translation and Destruction of Classified Information

1. All reproductions and translations shall bear appropriate security classification markings and they shall 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 ERITTÄIN SALAINEN/ STROGO TAJNO shall be translated or reproduced only upon the written permission of the Originating Party.

4. Classified Information marked ERITTÄIN SALAINEN/ STROGO TAJNO shall not be destroyed. It shall be returned to the Originating Party after it is no longer considered necessary by the Parties.

5. Information classified as SALAINEN/TAJNO or below shall be destroyed after it is no longer considered necessary by the Recipient Party, in accordance with national legislation.

Article 10

Classified Contracts

1. If the Competent Security Authority of the Originating Party intends to permit negotiations for concluding a Classified Contract with a contractor under the jurisdiction of the Recipient Party, it shall, on request, obtain all

få alla relevanta säkerhetsintyg av mottagarpartens behöriga säkerhetsmyndighet.

2. I fall det gäller ett öppet säkerhetsklassificerat anbudsförfarande kan mottagarpartens behöriga säkerhetsmyndighet även utan begäran överlämna de relevanta säkerhetsintygen till den utlämnande partens säkerhetsmyndighet.

3. Samma säkerhetskrav, relevanta intyg medräknade, ska tillämpas på underleverantörer som på den kontraktspart som har ingått det säkerhetsklassificerade huvudkontraktet.

4. Den utlämnande partens behöriga säkerhetsmyndighet kan föreslå och delta i säkerhetsinspektioner som mottagarpartens behöriga säkerhetsmyndighet gör för att säkerställa att deras anläggningar är i överensstämmelse med denna överenskommelse.

Artikel 11

Besök

1. Besök som kräver tillgång till säkerhetsklassificerad information kan tillåtas med skriftligt förhandstillstånd av värdlandets behöriga säkerhetsmyndighet.

2. Begäran om besök ska företes respektive behöriga säkerhetsmyndighet minst 20 dagar före besöket och den ska innehålla följande uppgifter:

- a) besökarens namn, födelsedatum och -ort, nationalitet och nummer på identitetsbevis eller pass,
 - b) besökarens ställning, med uppgift om vilken arbetsgivare besökaren företräder,
 - c) uppgifter om projektet besökaren är delaktig i,
 - d) giltighetstid och nivå på besökarens säkerhetsintyg, om så krävs,
 - e) namn, adress, telefon- eller faxnummer, e-postadress och kontaktperson på anläggningen som ska besökas,
 - f) besökets syfte och högsta säkerhetsklass i den berörda säkerhetsklassificerade informationen,
 - g) besökets tidpunkt och längd, vid upprepade besök period över vilken besöken sträcker sig,
 - h) datum och underteckning av den utlämnande partens behöriga säkerhetsmyndighet.
3. I brådskande fall kan de behöriga säker-

relevanta security certificates from the Competent Security Authority of the Recipient Party.

2. In the case of an open classified tender the Competent Security Authority of the Recipient Party may provide the Competent Security Authority of the Originating Party with the relevant security certificates even without a request.

3. Sub-contractors shall be subject to the same security requirements, including due certifications, as the contractor which concluded the main Classified Contract.

4. The Competent Security Authority of the Originating Party may propose and participate in security inspections carried out by the Competent Security Authority of the Recipient Party at facilities to ensure their compliance with this Agreement.

Article 11

Visits

1. Visits necessitating access to Classified Information shall be subject to prior permission of the Competent Security Authority of the host Party.

2. A request for visit shall be submitted to the relevant Competent Security Authority at least 20 days prior to the commencement of the visit and shall include the following:

- a) the visitor's name, date and place of birth, nationality and ID card/passport number;
 - b) the visitor's position, with a specification of the employer which the visitor represents;
 - c) a specification of the project in which the visitor participates;
 - d) the validity and level of the visitor's security clearance, if required;
 - e) the name, address, phone/fax number, e-mail and point of contact of the facility to be visited;
 - f) the purpose of the visit, including the highest level of Classified Information to be involved;
 - g) the date and duration of the visit. In the case of recurring visits the total period covered by the visits shall be stated;
 - h) the date and signature of the sending Competent Security Authority.
3. In urgent cases, the Competent Security

hetsmyndigheterna avtala om en kortare tidsfrist för begäran om besök.

4. De behöriga säkerhetsmyndigheterna kan avtala om att göra upp förteckningar över besökare med tillstånd till upprepade besök. Förteckningen ska till en början gälla i högst 12 månader och giltighetstiden kan förlängas med högst 12 månader. En begäran som gäller upprepade besök ska göras upp i enlighet med punkt 2. När en förteckning har godkänts kan respektive organisationer arrangera sina besök direkt sinsemellan.

5. Säkerhetsklassificerad information som en besökare förvärvar ska anses som säkerhetsklassificerad information i enlighet med denna överenskommelse.

Artikel 12

Säkerhetssamarbete

1. För att få till stånd och kunna upprätthålla sinsemellan jämförbara säkerhetsnivåer ska de behöriga säkerhetsmyndigheterna på begäran underrätta varandra om sina nationella säkerhetsnormer och -förfaranden och sin praxis för skydd av säkerhetsklassificerad information. De behöriga säkerhetsmyndigheterna får besöka varandra i detta syfte.

2. De behöriga säkerhetsmyndigheterna ska underrätta varandra om exceptionella säkerhetsrisker som kan äventyra sekretessen i utlämnad säkerhetsklassificerad information.

3. På begäran ska de behöriga säkerhetsmyndigheterna i enlighet med nationell lagstiftning bistå varandra i förfaranden i anslutning till säkerhetsutredningar.

4. De behöriga säkerhetsmyndigheterna ska utan dröjsmål underrätta varandra om ändringar som gäller ömsesidigt erkända säkerhetsintyg.

5. De fördragsslutande parternas säkerhetsmyndigheter kan direkt sinsemellan utbyta operativa eller underrättelseuppgifter i enlighet med nationell lagstiftning.

6. Samarbetet som sker med stöd av denna överenskommelse ska föregå på engelska.

Artikel 13

Sekretessbrott

1. De fördragsslutande parterna ska utan

Authorities can agree on a shorter period.

4. The Competent Security Authorities may agree on a list of visitors entitled to recurring visits. The list shall be valid for an initial period not exceeding 12 months and may be extended for a further period of time not exceeding 12 months. A request for recurring visits shall be submitted in accordance with Paragraph 2 of this Article. Once a list has been approved, visits may be arranged directly between the facilities involved.

5. Any Classified Information acquired by a visitor shall be considered as Classified Information under this Agreement.

Article 12

Security co-Operation

1. 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 security standards, procedures and practices for the protection of Classified Information. To this aim the Competent Security Authorities may visit each other.

2. The Competent Security Authorities shall inform each other of exceptional security risks that may endanger the released Classified Information.

3. On request, the Competent Security Authorities shall, in accordance with national legislation, assist each other in carrying out security clearance procedures.

4. The Competent Security Authorities shall promptly inform each other about any changes in mutually recognized security clearances.

5. The security services of the Parties may exchange operative and/or intelligence information directly in accordance with national legislation.

6. The co-operation under this Agreement shall be effected in the English language.

Article 13

Breach of Security

1. Each Party shall immediately notify the

dröjsmål underrätta varandra om misstänkta eller upptäckta fall av sekretessbrott eller äventyrande av sekretessen i säkerhetsklassificerad information.

2. Den behöriga fördragsslutande parten ska i enlighet med sin nationella lagstiftning vidta alla de relevanta åtgärder som är möjliga för att begränsa följderna av sekretessbrottet eller äventyrandet av sekretessen som avses i första stycket och för att förhindra fortsatta sekretesskränkningar. På begäran ska den andra parten bistå undersökningen, få besked om dess resultat och om vilka åtgärder som har vidtagits på grund av kränkningen.

Artikel 14

Kostnader

Vardera fördragsslutande parten ska själv stå för de kostnader som orsakas dem av genomförandet av denna överenskommelse.

Artikel 15

Tolkning och lösning av tvister

Tvister som uppkommer angående tolkning eller tillämpning av överenskommelsen ska uteslutande avgöras i samråd mellan parterna.

Artikel 16

Slutbestämmelser

1. Denna överenskommelse gäller för obestämd tid. Den ska godkännas i enlighet med de fördragsslutande parternas nationella rättsliga förfaranden och den träder i kraft den första dagen den andra månaden efter att den senare underrättelsen mellan parterna om att kraven för överenskommelsens ikraftträdande har uppfyllts har tagits emot.

2. Vardera fördragsslutande parten har rätt att när som helst skriftligt säga upp överenskommelsen. Då upphör överenskommelsen att gälla sex månader efter den dag, då den andra fördragsslutande parten har mottagit meddelandet om uppsägning.

3. Utan hinder av en uppsägning ska all säkerhetsklassificerad information som har ut-

other Party of any suspicion or discovery of a breach or compromise of the security of Classified Information.

2. The competent Party shall undertake all possible appropriate measures under its national legislation so as to limit the consequences of the breach or compromise referred to in Paragraph 1 of this Article and to prevent further violations. On request, the other Party shall provide investigative assistance; it shall be informed of the outcome of the investigation and the measures undertaken due to the violation.

Article 14

Expenses

Each Party shall bear its own expenses incurred in the course of implementation of this Agreement.

Article 15

Interpretation and Dispute Settlement

Any dispute between the Parties on the interpretation or application of this Agreement shall be re-solved exclusively by means of consultation between the Parties.

Article 16

Final Provisions

1. This Agreement is concluded for an indefinite period of time. It is subject to approval in accordance with the national legal procedures of the Parties and shall enter into force on the first day of the second month following receipt of the later notification between the Parties that the necessary requirements for this Agreement to enter into force have been met.

2. Each Party shall have the right to terminate this Agreement in writing at any time. In such a case the validity of the Agreement shall expire 6 months following the day on which the termination notice was received by the other Party.

3. Notwithstanding the termination of this Agreement, all Classified Information deliv-

lämnats i enlighet med överenskommelsen fortsättningsvis skyddas i enlighet med överenskommelsens bestämmelser, tills den utlämnande parten befriar mottagarparten från denna skyldighet.

4. Denna överenskommelse kan med skriftligt samtycke av de fördragsslutande parterna när som helst ändras. Ändringar träder i kraft i enlighet med punkt 2.

5. Denna överenskommelse inverkar inte på de fördragsslutande parternas rättigheter och skyldigheter utgående från andra internationella överenskommelser.

6. Verkställighetsåtgärder för att genomföra överenskommelsen kan vidtas.

Upprättad i Ljubljana den 6 maj 2008 i två original, båda på finska, slovenska och engelska språken, vilka alla texter är lika giltiga. I fall av skiljaktigheter i tolkningen ska den engelska texten ha företräde.

Till bekräftelse av vilket de undertecknade, därtill vederbörligen befullmäktigade, har undertecknat denna överenskommelse.

För Republiken
Finlands regering

För Republiken
Sloveniens regering

ered under this Agreement shall continue to be protected in accordance with the provisions stated in this Agreement until the Originating Party dispenses the Recipient Party from this obligation.

4. This Agreement may be amended at any time by written consent of both Parties. Such amendments shall enter into force in accordance with Paragraph 1 of this Article.

5. This Agreement does not prejudice the rights and obligations of the Parties arising from other international agreements.

6. Implementing arrangements may be concluded for the implementation of this Agreement.

Done in on in two originals in the Finnish, Slovenian and English languages, each text being equally authentic. In case of different interpretation the English text shall prevail.

In witness whereof the undersigned, being duly authorised thereto, have signed this Agreement.

On behalf of the Government of the
Republic of Finland

On behalf of the Government of the
Republic of Slovenia