

Regeringens proposition till Riksdagen om godkännande av överenskommelsen mellan Finland och Estland om ömsesidigt skydd för 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 Estland om ömsesidigt skydd för 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 Estland i utrikes-, försvars-, säkerhets-, polis- och industriärenden. Det är fråga om känsligt informationsmaterial 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 NULÄGET	4
2.1 Lag om internationella förpliktelser som gäller informationssäkerhet	4
2.2 Lagstiftning om säkerhetsutredningar	7
3 MÅLSÄTTNING	7
4 PROPOSITIONENS KONSEKVENSER	7
4.1 Konsekvenser för medborgarna	7
4.2 Konsekvenser för näringslivet	8
4.3 Ekonomiska konsekvenser	8
4.4 Konsekvenser för förvaltningen	8
5 BEREDNINGEN AV PROPOSITIONEN	8
DETALJMOTIVERING	9
1 ÖVERENSKOMMELSENS INNEHÅLL OCH FÖRHÅLLANDE TILL LAGSTIFTNINGEN I FINLAND.....	9
2 LAGFÖRSLAG	13
3 IKRAFTTRÄDANDE	13
4 BEHOVET AV RIKSDAGENS SAMTYCKE SAMT BEHANDLINGSORDNING ..	14
4.1 Behovet av riksdagens samtycke	14
4.2 Behandlingsordning	15
LAGFÖRSLAG	17
Lag om sättande i kraft av de bestämmelser i överenskommelsen med Estland om ömsesidigt skydd för säkerhetsklassificerad information som hör till området för lagstiftningen	17
FÖRDRAGSTEXT	18

ALLMÄN MOTIVERING

1 Inledning

Med informationssäkerhet avses allmänt taget alla förfaranden som skyddar informationsinnehållet gentemot utomstående (informationens konfidentialitet), informationens oförändrbarhet (integritet) samt informationens användbarhet. För att trygga informationssäkerheten används olika metoder av vilka 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 inhämtande, 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 handlar om Finlands trovärdighet som part i det internationella samarbetet.

Det internationella informationssäkerhets-samarbetet, som även Finland är delaktig i, omfattar sedan vanligt 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 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 kutymmer, 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 stora medlemsländer 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 94-95/2004). 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 anbudsförfaranden.

Finland har hitintills, utöver överenskommelsen med Estland, undertecknat informationssäkerhetsöverenskommelser med Polen, Italien, Slovakien och Lettland. Avtalen med Spanien, Tjeckien och Litauen har framskridit till paraferingsskedet, liksom även den samnordiska informationssäkerhetsöverenskommelsen.

Överenskommelsen mellan Finland och Estland undertecknades i Tallinn den 5 juni 2007. Den har till största delen förhandlats fram utgående från ett modellavtal som Finland lade fram som underlag för förhandlingarna.

2 Nuläget

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 behövlig bl.a. för att det i samband med att internationella överenskommelser sätts i kraft är nödvändigt att avvika från våra nationella regleringar som utgår från handlingars offentlighet och säkerhet, i huvudsak med stöd av 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 tillämpas endast om den internationella överenskommelsen har satts i kraft i Finland på det sätt som grundlagen förutsätter 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 information om särskilt känsligt material begärs med stöd av offentlighetslagen. 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 ge den information som behövs 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 skyddet för säkerhetsklassificerad information har äventyrats eller om bestämmelser om informationssäkerhet har överträtts, samt vidta åtgärder för att utreda ärendet och väcka åtal mot de skyldiga (19 §).

Sekretessbeläggning och reglering av användningen av information

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 överlätas 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 utrymmen (10 §).

I lagen om internationella förpliktelser som gäller informationssäkerhet har skrivits in det i internationella överenskommelser allmänna kravet att myndigheterna ska iaktta stor restriktivitet vid användningen 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 såvida detta förutsätts i överenskommelsen. Detsamma gäller näringsidkare, så som avses i 1 § 2 mom. (6 § 3 mom.).

Personssäkerhet

Sådan personssäkerhetsutredning 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 utredning är nödvändig för att fullgöra en in-

ternationell 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 skyddspolis (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 säkerhetsmyndigheten eller, om så har överenskommit mellan säkerhetsmyndigheterna, av den för uppgiften utsedda säkerhetsmyndigheten.

Det utfärdas ett personligt säkerhetsintyg (Personal Security Clearance) över bedömningen. 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 skall 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 upplysningar om huruvida en säkerhetsutredning som gäller en själv har gjorts med tanke på ett visst 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 Estland och så förbättra samarbetet mellan länderna samt att trygga finländska företags möjligheter att delta i internationella eller finsk-estniska 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 Estland till Finland. I lagen ingår en specialbestämmelse om att handlingar, och informationen de innehåller, som hos den andra fördragslutande 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 informa-

tionssäkerhet har sålunda en mera heltäckande ordalydelse än den allmänna offentlighetslagen.

Överenskommelsen mellan Finland och Estland gäller handlingar som den ena fördragsslutande parten anser att skall 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 skall 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 den rätta eller om vilken information i handlingen det är som föranleder klassificeringen, skall myndigheten kontakta den fördragsslutande part som har upprättat handlingen. En uttrycklig bestämmelse om detta ingår i artikel 3.1 i överenskommelsen mellan Finland och Estland.

Med stöd av det som anförs ovan kan bedömningen göras att förslaget om att sätta i kraft överenskommelsen om informationssäkerhet mellan Finland och Estland 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 möjligheter för den finländska industrin till att i motsats till tidigare få beställningar eller delta i projekt som förutsätter tillgång till information som är säkerhetsklassificerad i Estland. Analogt öppnar överenskommelsen möjligheter för den estniska industrin till att i motsats till tidigare få beställningar eller 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 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 handels- och industriministeriet.

Utlåtanden om propositionen har begärts av justitieministeriet, handels- och industriministeriet, försvarsministeriet, finansministeriet, inrikesministeriet, kommunikationsministeriet, skyddspolisen, huvudstaben samt Industrin och arbetsgivarna rf.

I utlåtandena förordas ett snabbt godkännande och ikraftsättande av överenskommelsen.

DETALJMOTIVERING

1 Överenskommelsens innehåll och förhållande till lagstiftningen i Finland

Artikel 1. Tillämpningsområde. I artikeln definieras att syftet med överenskommelsen är att skydda säkerhetsklassificerad information som Finland och Estland förmedlar till varandra. Den allmänna skyddsförpliktelsen anges i artikel 3.1, enligt vilken de fördragsslutande parterna förbinder sig att ge säkerhetsklassificerad information som de förmedlat till varandra samma skydd som de ger eget nationellt informationsmaterial av motsvarande säkerhetsklass.

I artikel 1 i överenskommelsen definieras de funktioner som överenskommelsen skall tillämpas på. Dessa är utrikes-, försvars-, säkerhets-, polis- och industriärenden. Upprätthållandet av gränssäkerheten anses ingå i dessa ärenden. 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 2. Definitioner. I artikeln definieras de för tillämpningen av överenskommelsen centrala begreppen.

I punkt a definieras säkerhetsklassificerad information. Överenskommelsen gäller information eller material som har säkerhetsklassificerats i enlighet med den fördragsslutande partens nationella lagstiftning.

I punkt b definieras som kontraktspart en fysisk eller juridisk person eller myndighet som hör till en fördragsslutande parts jurisdiktion och har behörighet att ingå kontrakt.

I punkt c definieras ett säkerhetsklassificerat kontrakt. Det är frågan om ett kontrakt mellan två eller flera kontraktsparter, vilket för att kunna fullgöras kräver tillgång till eller användning av säkerhetsklassificerad information, eller där säkerhetsklassificerad information framställs för att fullgöra kontraktet eller uppkommer på grund av kontraktet. Punkten är i samklang med 2 § 3 punkten i lagen om internationella förpliktelser som gäller informationssäkerhet.

Enligt punkt d avses med nationell säkerhetsmyndighet en nationell myndighet som har ansvar för genomförandet och övervakningen av överenskommelsen.

I punkt e definieras en behörig myndighet som en nationell säkerhetsmyndighet eller annan nationell myndighet som med stöd av den nationella lagstiftningen har ansvar för att genomföra överenskommelsen.

I punkt f definieras en utlämnande part som den fördragsslutande part, från vilken den säkerhetsklassificerade informationen härrör. Det handlar alltså om ägaren till den säkerhetsklassificerade informationen. Definitionen omfattar såväl staten och inrättningar som hör till dess jurisdiktion som offentlig- och privaträttsliga juridiska personer.

Enligt punkt g avses med en mottagarpart den fördragsslutande part, till vilken den säkerhetsklassificerade informationen förmedlas. Definitionen omfattar såväl staten och inrättningar som hör till dess jurisdiktion som offentlig- och privaträttsliga juridiska personer.

Enligt punkt h avser nationell lagstiftning lagar, författningar på lägre nivå samt myndighetsbestämmelser och -föreskrifter.

I punkt i definieras säkerhetsintyg baserade på en personsäkerhetsutredning som en bedömning, utförd av behörig myndighet i enlighet med den nationella lagstiftningen, med vilken en person ges rätt att få tillgång till säkerhetsklassificerad information.

I punkt j definieras ett säkerhetsintyg baserat på en säkerhetsutredning som gäller sammanslutning som en handling, med vilken intygas att en juridisk person och dennas lokaler har vederbörlig fysisk och organisatorisk beredskap att använda och deponera säkerhetsklassificerad information i enlighet med relevant nationell lagstiftning.

Enligt punkt k avses med informationsbehov ett verifierat behov av säkerhetsklassificerad information. Definitionen motsvarar bestämmelserna i 6 § 3 mom. i lagen om internationella förpliktelser som gäller informations säkerhet.

Artikel 3. Skydd av säkerhetsklassificerad information. I artikel 3.1 anges den centrala principen i överenskommelsen, enligt vilken de fördragsslutande parterna förbinder sig att

ge säkerhetsklassificerad information samma skydd de ger egen information av motsvarande säkerhetsklass.

I artikel 3.2 förbjuds överlåtelse av säkerhetsklassificerad information till internationella organisationer eller tredje stater, medräknat deras tjänstemän, medborgare och juridiska personer utan avsändarens skriftliga tillstånd. 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 informations-säkerhet skall sekretessbeläggas.

Enligt artikel 3.3 får säkerhetsklassificerad information användas endast för det ändamål avsändaren har angett. Förpliktelsen motsvaras av bestämmelsen i 6 § 2 mom. i lagen om internationella förpliktelser som gäller informations-säkerhet.

I artikel 3.4 föreskrivs att fysiska personer får ges tillgång till säkerhetsklassificerad information endast för skötseln av deras arbete eller utförandet av ett givet uppdrag, utgående från ett verifierat informationsbehov.

Artikel 3.5 gör det möjligt att ge tillgång till information som har klassificerats som KONFIDENTIELL/KONFIDENTSIAALNE eller högre endast till fysiska personer som har säkerhetsklarerats. Bestämmelsen är i samklang med 6 § 3 mom. i lagen om internationella förpliktelser som gäller informationssäkerhet, enligt vilken endast personer som behöver informationen för skötseln av sina uppgifter ska ha tillgång till det. Den kontroll av personers tillförlitlighet som den internationella informations-säkerhetsförpliktelsen förutsätter görs i Finland i enlighet med lagen om säkerhetsutredningar samt enligt 11 § i lagen om internationella förpliktelser som gäller informations-säkerhet. Huvudstaben svarar för att säkerhetsutredningar görs i ärenden som gäller försvarsförvaltningen, i övriga fall görs utredningarna av skyddspolis.

I artikel 3.6 förpliktas de fördragsslutande parterna se till att säkerhetsutredningarna av såväl sammanslutningar som personer sker på vederbörligt sätt.

Artikel 4. Säkerhetsklasserna. I artikel 4.1 definieras hur de finländska och estniska sä-

kerhetsklasserna motsvarar varandra. Bägge stater har fyra säkerhetsklasser.

Den högsta säkerhetsklassen, som kräver de strängaste informations-säkerhetsåtgärderna, är "YTTERST HEMLIG" (TÄIESTI SALAJANE). Till denna klass 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 "HEMLIG" (SALAJANE). Till denna klass 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" (KONFIDENTSIAALNE), 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" (PIIRATUD), hör information som, om den obehörigen röjs, kan skada allmänna intressen eller försämra myndigheternas möjligheter att agera.

I artikel 4.2 förpliktas en fördragsslutande part att förse mottagen säkerhetsklassificerad information med sin egen motsvarande klassificeringsanteckning i enlighet med den i artikel 4.1 föreskrivna motsvarighetsskalan. I 8 § i lagen om internationella förpliktelser som gäller informations-säkerhet föreskrivs om anteckningsskyldighet.

Artikel 4.3 handlar om mottagarpartens skyldighet att bevara den mottagna informationens säkerhetsklass. Mottagarpartens säkerhetsmyndighet har endast på begäran av den utlämnande partens behöriga säkerhetsmyndighet rätt att ändra eller upphäva klassificeringsanteckningen.

I artikel 4.4 konstateras att mottagarpartens säkerhetsmyndighet har rätt att be om att få

ändra eller häva en klassificeringsanteckning. Denna punkt är viktig när en finländsk myndighet får en begäran om information som ingår i en säkerhetsklassificerad handling. Myndigheten skall enligt bestämmelserna i 17 § i offentlighetslagen se till att tillgången till information inte begränsas mera än vad som är nödvändigt för intresset som skall skyddas. Om det till exempel på grund av tidens gång inte längre tycks finnas grund för säkerhetsklassificeringen av en begärd handling borde myndigheten för att kontrollera klassificeringen kontakta den estniska säkerhetsmyndigheten som vid behov kan besluta om en ändring av handlingens säkerhetsklassificering.

Artikel 5. Säkerhetsklassificerade kontrakt. Artikeln innehåller de bestämmelser som ska tillämpas när den utlämnande parten ingår eller tillåter en kontraktspart inom sin egen jurisdiktion att ingå ett säkerhetsklassificerat kontrakt som avses i artikel 2 punkt c med en kontraktspart som hör till den andra fördragslutande slutande partens jurisdiktion.

Enligt artikel 5.1 ska den utlämnande partens säkerhetsmyndighet av mottagarpartens säkerhetsmyndighet erhålla ett säkerhetsintyg över kontraktsparten baserat på en säkerhetsutredning som gäller sammanslutning. När det gäller ett anbudsförfarande måste intyget lämnas in förrän säkerhetsklassificerad information överläts till den som vill delta i ett anbudsförfarande.

I artikel 5.2 föreskrivs att säkerhetsklassificerade kontrakt ska inbegripa en särskild säkerhetsklausul.

I artikel 5.3 förutsätts att de behöriga myndigheterna ska säkerställa att säkerhetsklassificerade kontrakt innehåller bestämmelser om förbud att ingå säkerhetsklassificerade kontrakt med underleverantörer innan den behöriga myndigheten har gett sitt tillstånd. Underleverantörer jämföras med huvudkontraktets kontraktsparter vad kraven på informationssäkerhet beträffar.

Artikel 5.4 innehåller en förteckning över de åtgärder de behöriga myndigheterna ska vidta innan en kontraktspart ges tillgång till säkerhetsklassificerad information. Dessa åtgärder är att säkerställa att säkerhetsklassificerad information skyddas på vederbörligt sätt (punkt a), att säkerhetsintyg baserade på personsäkerhetsutredningar utfärdas till personer som har

ett verifierat behov av tillgång till säkerhetsklassificerad information i sitt arbete eller för ett givet uppdrag (punkt b), att säkerställa att alla som har tillgång till säkerhetsklassificerad information är medvetna om sina skyldigheter i enlighet med tillämplig nationell lagstiftning (punkt c) samt att utföra säkerhetsgranskningar i de lokaler övervakningsskyldigheten gäller (punkt d).

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. Den för att uppfylla förpliktelsen nödvändiga rätten för finländska myndigheter att lämna ut information finns förskrivna i 17 § i lagen om internationella förpliktelser som gäller informationssäkerhet.

Artikel 6. Förmedling av säkerhetsklassificerad information. Artikel 6.1 och 6.2 innehåller bestämmelser om förfarandet vid förmedling av säkerhetsklassificerad information mellan de fördragsslutande parterna. Vilka metoder som används vid förmedlingen beror på informationens säkerhetsklass. Information som hör till säkerhetsklassen YTTERST HEMLIG/TÄIESTI SALAJANE förmedlas endast via officiella regeringskanaler. Likaledes ska information i säkerhetsklasserna HEMLIG/SALAJANE och KONFIDENTIELL/KONFIDENTSIAALNE sändas via officiella regeringskanaler, men i brådskande fall eller i fråga om särskilt angivna projekt eller program kan sådan information med tillstånd av de behöriga säkerhetsmyndigheterna även förmedlas via andra kanaler.

Artikel 6.3 innehåller bestämmelser om de tekniska skyldigheterna i anslutning till förmedling av information som hör till säkerhetsklassen KONFIDENTIELL/KONFIDENTSIAALNE eller högre, såsom om kravet på personsäkerhetsintyg för kuriren (punkt a), om ett sändningsregister som den utlämnande parten ska föra och om mottagarpar-

tens rätt att få utdrag ur detta register (punkt b), om förpackning och försegling av materialet (punkt c) samt om skriftliga mottagningsbekräftelser (punkt d).

Artikel 6.4 ger de behöriga myndigheterna rätt att avtala om specialarrangemang för större materialförsändelser.

Artikel 6.5 ger rätt att sända information som hör till säkerhetsklassen BEGRÄNSAD TILLGÅNG/PIIRATUD per post eller med någon annan leveransservice.

Enligt artikel 6.6 får säkerhetsklassificerad information förmedlas elektroniskt endast med användning av metoder som de behöriga myndigheterna gemensamt har godkänt och i fullt krypterad form.

Artikel 6.7 ger de fördragsslutande parternas säkerhetstjänster rätt till utbyte av operativ information eller underrättelseuppgifter i enlighet med nationell lagstiftning.

Artikel 7. Översättning, kopiering och utplåning av säkerhetsklassificerad information. Artikel 7 innehåller bestämmelser om hur material som hör till de olika säkerhetsklasserna får översättas, kopieras och utplånas.

Artikel 7.1 innehåller ett förbud mot översättning och kopiering av information som hör till de två högsta säkerhetsklasserna utan skriftligt förhandstillstånd av den utlämnande partens säkerhetsmyndighet. Nationella bestämmelser om hur förpliktelsen ska uppfyllas kan vid behov utfärdas med stöd av 9 § i lagen om internationella förpliktelser som gäller informationssäkerhet.

Enligt 7.2 ska information som hör till säkerhetsklass HEMLIG/SALAJANE eller KONFIDENTIELL/KONFIDENTSIAALNE returneras till avsändaren eller utplånas i enlighet med den nationella lagstiftningen.

Enligt 7.3 ska information i säkerhetsklass YTTERST HEMLIG/TÄIESTI SALAJANE i enlighet med den nationella lagstiftningen returneras till den utlämnande parten när det anses att den inte längre behövs. Hänvisningen till den nationella lagstiftningen avser situationer där materialet eller en del av det på grund av arkiveringslagstiftningen skall sparas.

Enligt 7.4 ska säkerhetsklassificerad information i krissituationer, där säkerhetsklassificerad information som har framställts eller överförs i enlighet med överenskommelsen inte kan skyddas eller returneras, omedelbart

utplånas. Mottagarparten ska så fort som möjligt underrätta den utlämnande partens nationella säkerhetsmyndighet om att säkerhetsklassificerad information har utplånats.

Artikel 8. Besök. Artikel 8 innehåller bestämmelser om de förfaringssätt som ska följas när man bereder den utlämnande partens myndigheter tillfälle att utföra säkerhetsgranskningar i mottagarpartens lokaler eller vid besök av de fördragsslutande parternas anställda i sådana lokaler som hör till de fördragsslutande parterna där säkerhetsklassificerad information framställs, hanteras eller förvaras eller där man genomför säkerhetsklassificerade projekt. Avsikten med besök av de fördragsslutande parternas företrädare är att säkerställa att överenskommelsens syfte uppfylls och säkerhetsklassificerad information skyddas på ett vederbörande sätt.

Enligt 8.1 ska mottagarparten tillåta säkerhetsgranskningar, men endast av personer med personsäkerhetsintyg.

Enligt bestämmelserna i artikel 8.2–8.5 ska en fördragsslutande part tillåta besök av den andra fördragsslutande partens anställda, under förutsättning att besökarna iakttar de nationella säkerhetsbestämmelserna. Klassificerad information som har överlåtits till sådana besökare anses ha överlåtits till den andra fördragsslutande parten. När det gäller information i säkerhetsklassen

KONFIDENTIELL/KONFIDENTSIAALNE eller högre ska besöksansökan tillställas mottagarparten via officiella regeringskanaler och begränsas till besök som gäller företagssäkerhet eller säkerhetsgranskningar. Besöksansökan ska innehålla de i bilagan till överenskommelsen specificerade uppgifterna om besökaren och besöksobjektet och göras upp på den fördragsslutande partens nationella språk eller på engelska minst två veckor före den planerade tidpunkten för besöket.

Enligt 8.6 kan säkerhetsmyndigheterna för att underlätta sitt praktiska arbete göra upp en förteckning över personer som har tillstånd till multipla besök i anslutning till ett säkerhetsklassificerat projekt. Förteckningarna ska göras upp i enlighet med den nationella lagstiftningen på det sätt som konstateras i artikel 8.7. När en förteckning har gjorts upp kan detaljerna kring ett enskilt besök avtalas direkt med den kontraktspart eller organisation som ska

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

Artikel 9. Underrättelser och samråd. Artikeln innehåller bestämmelser om samarbetet mellan fördragsslutande parternas myndigheter för att säkerställa att överenskommelsen blir genomförd.

Enligt 9.1 ska de fördragsslutande parternas behöriga säkerhetsmyndigheter informera varandra om nationell lagstiftning som är relevant för genomförande av överenskommelsen och om eventuella ändringar i den (punkt a) samt om de nationella säkerhetsmyndigheterna och ändringar som gäller dem (punkt b). Enligt lagen om internationella förpliktelser som gäller informationssäkerhet är utrikesministeriet nationell säkerhetsmyndighet (National Security Authority, NSA) i Finland, och uppgiften handhas av säkerhetsenheten. Estlands nationella säkerhetsmyndighet är försvarsministeriet.

I artikel 9.2 fastställs de behöriga säkerhetsmyndigheternas inbördes samrådspålit på någönderas initiativ.

Artikel 10. Tvistlösning. Enligt artikeln ska alla tvister som uppkommer mellan de fördragsslutande parterna om tolkning eller tillämpning av överenskommelsen avgöras endast och enbart i samråd mellan de fördragsslutande parterna.

Artikel 11. Kränkningar av sekretessbestämmelserna för säkerhetsklassificerad information. I artikel 11.1 förpliktas de fördragsslutande parterna att utan dröjsmål underrätta varandra om misstänkta eller upptäckta fall av kränkning eller äventyrande av sekretessen i säkerhetsklassificerad information. I artikel 11.2 förpliktas de fördragsslutande parterna att i enlighet med sin nationella lagstiftning vidta alla åtgärder som fordras för att begränsa konsekvenserna av sådana kränkningar och för att förhindra att kränkningarna fortgår. De fördragsslutande parterna förpliktas också att på begäran bistå varandra i undersökningarna och att underrätta varandra om undersökningarnas resultat och vidtagna åtgärder. Nödvändiga bestämmelser för att genomföra de förpliktelser som avses i artikeln ingår i 19 § i lagen om internationella förpliktelser som gäller informationssäkerhet.

Artikel 12. Kostnader. Enligt artikeln ska bägge fördragsslutande parter själva stå för de kostnader som förorsakas dem av genomförandet av överenskommelsen.

Artikel 13. Slutbestämmelser. I artikeln föreskrivs om ikraftträdandet av överenskommelsen, ändringar i den samt uppsägning av den. Överenskommelsen ska gälla tills vidare och den kan ändras med en skriftlig överenskommelse mellan de fördragsslutande parterna.

Bilaga Besöksansökan

Överenskommelsen har en bilaga där de uppgifter räknas upp i detalj som en fördragsslutande part ska inkludera i besöksansökan som anges i artikel 8 i överenskommelsen.

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

1 §. Genom bestämmelsen i lagförslagens 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 13.1 i överenskommelsen mellan Finland och Estland ska de fördragsslutande parterna underrätta varandra när de åtgärder som den nationella lagstiftningen kräver för att

sätta i kraft överenskommelsen har slutförts. 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 samt 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 förutsätter flera bestämmelser i den överenskommelse som ingår i propositionen riksdagens samtycke. I artikel 1 definieras överenskommelsens syfte och tillämpningsområde. I artikel 2 definieras vad som avses med säkerhetsklassificerad information och säkerhetsklassificerat kontrakt. Eftersom dessa bestämmelser i överenskommelsen direkt eller indirekt påverkar tolkningen och tillämpningen av materiella bestämmelser som hör till området för lagstiftningen förutsätter de riksdagens godkännande (GrUU 6/2001 rd).

I artikel 3 föreskrivs om åtgärder som fordras för ömsesidigt skydd av säkerhetsklas-

sificerad information inom överenskommelsens tillämpningsområde och som begränsar förmedling och användning av samt tillgången till säkerhetsklassificerad information. I artikel 3.1 förpliktas de fördragsslutande parterna att i enlighet med sin nationella lagstiftning vidta de åtgärder som fordras för att på vederbörligt sätt skydda sådan säkerhetsklassificerad information som avses i överenskommelsen. De fördragsslutande parterna är skyldiga att ge denna säkerhetsklassificerade information samma skydd som de ger egen information av motsvarande säkerhetsklass. Enligt artikel 3.2 ska mottagarparten i regel sekretessbelägga säkerhetsklassificerad information. I Finland är myndighetshandlingarna 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 anteckning om sekretess göras i en myndighetshandling som en myndighet ger ut till en part och som ska vara sekretessbelagd på grund av någon annans eller allmänt intresse. I andra sekretessbelagda handlingar kan 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. I enlighet med den ska särskilt känsligt informationsmaterial oberoende av vad som föreskrivs i lagen om offentlighet i myndigheternas verksamhet föras 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 förutsätter riksdagens samtycke. I artikel 3.3 anges en begränsning i användningen av säkerhetsklassificerad information och i 3.4 och 3.5 en begränsning i personers tillgång till säkerhetsklassificerad in-

formation. En fördragsslutande part har rätt att överlåta information endast till personer som har ett informationsbehov för skötseln av sitt arbete eller för utförandet av ett givet uppdrag och vid behov ett säkerhetsintyg baserat på en personsäkerhetsutredning. I artikel 3.6 föreskrivs om de fördragsslutande parternas skyldighet att säkerställa att lokalerna säkerhetsgranskas samt personsäkerhetsutredningarna görs på vederbörligt sätt. I upplägget för säkerhetsutredningar ska beaktas vad som sägs i 10 § 1 mom. i grundlagen om tryggt privatliv och om plikten att lagstifta om skydd för personuppgifter. I Finland finns det föreskrifter om personer som är föremål för säkerhetsutredningar samt om utredningsförfarandet i lagen om säkerhetsutredningar. Om säkerhetskraven på utrymmen finns det bestämmelser i 10 § i lagen om internationella förpliktelser som gäller informationssäkerhet.

I artikel 5 i överenskommelsen finns det bestämmelser om säkerhetsklassificerade kontrakt och om säkerhetsutredningar som gäller de företag som är parter i sådana kontrakt. Föreskrifter om säkerhetsutredningar som gäller sammanslutningar ingår i 12 och 13 § i lagen om internationella förpliktelser om informationssäkerhet.

I artikel 6 finns det bestämmelser om förmedling av säkerhetsklassificerad information och i artikel 7 om översättning, kopiering och utlåning 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 beaktas i hanteringen av särskilt känsligt informationsmaterial kan utfärdas genom förordning av statsrådet.

I artikel 8 i överenskommelsen finns det bestämmelser om att en fördragsslutande part ska tillåta att representanter för den andra fördragsslutande parten eller för beställningsmottagare som verkar inom den partens territorium besöker partens egna offentliga myndigheter och inrättningar samt lokalerna till beställningsmottagare som är etablerade inom det egna territoriet. Avsikten med besök av de fördragsslutande parternas representanter är att säkerställa att överenskommelsens syfte att på ett adekvat sätt skydda 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 11 i överenskommelsen förutsätts att de fördragsslutande parterna omedelbart underrättar varandra såvida sekretessen i säkerhetsklassificerad information har överträtts eller om sådan information har utsatts för annan i artikeln nämnd kränkning. De fördragsslutande parterna ska också utreda överträdelser av sekretessbestämmelserna för säkerhetsklassificerad information samt vidta åtgärder för att förebygga sådana överträdelser. 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 3 artikel som ställer begränsningar för offentligheten när det gäller information och material som har säkerhetsklassificerats. Bestämmelsen är betydelsefull för den på offentlighetsprincipen baserade rätten till information som tryggas genom grundlagens 12 § 2 mom. Rätten till information får begränsas endast genom lag och endast av tvingande skäl. Att trygga Finlands och finländska företags möjligheter att delta i internationella samt finsk-estniska bilaterala aktiviteter och projekt som förutsätter utbyte av känslig och sekretessbelagd information kan anses vara ett sådant tvingande skäl. En specialbestämmelse om sekretessbeläggning ingår i 6 § i lagen om internationella förpliktelser som gäller informationssäkerhet.

Den mellan Finland och Estland ingångna överenskommelsen om ömsesidigt skydd för säkerhetsklassificerad information kan inte an-

ses 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 anføres ovan och i enlighet med grundlagens 94 § föreslås

att Riksdagen godkänner den i Tallinn den 5 juni 2007 mellan republiken Finland och republiken Estland ingångna överenskommelsen om ömsesidigt skydd för 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 Estland om ömsesidigt skydd för 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 Tallinn den 5 juni 2007 ingångna överenskommelsen mellan republiken Finland och republiken Estland om ömsesidigt skydd för säkerhetsklassificerad infor-

mation gäller som lag sådana Finland har förbundit sig till dem.

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

Helsingfors den 26 oktober 2007

Republikens President

TARJA HALONEN

Utrikesminister *Ilkka Kanerva*

ÖVERENSKOMMELSE

**mellan
Republiken Finlands regering
och
Republiken Estlands regering
om
ömsesidigt skydd för säkerhetsklassificerad information**

Republiken Finlands regering och Republiken Estlands regering, nedan "de fördragsslutande parterna", som önskar få till stånd ett arrangemang för ömsesidigt skydd av säkerhetsklassificerad information,

har kommit överens om följande:

Artikel 1*Syfte och tillämpningsområde*

Syftet med denna överenskommelse är att skydda säkerhetsklassificerad information som de fördragsslutande parterna förmedlar till varandra framför allt i samband med utrikes-, försvars-, säkerhets-, polis- eller industriärenden eller som förmedlas för att bereda eller fullgöra säkerhetsklassificerade kontrakt, eller som framställs utgående från eller som uppkommer på grund av förmedlad säkerhetsklassificerad information.

Artikel 2*Definitioner*

I denna överenskommelse avses med

a) säkerhetsklassificerad information: sekretessbelagd information eller sekretessbelagt material som förmedlas eller framställs i enlighet med denna överenskommelse och som har försetts med anteckning om säkerhetsklass i enlighet med den nationella lagstiftningen;

b) kontraktspart: fysisk eller juridisk person eller myndighet som hör till en fördragsslutande

AGREEMENT

**between
the Government of the Republic of
Finland
and
the Government of the Republic of Estonia
on the
Mutual Protection of Classified
Information**

The Government of the Republic of Finland and the Government of the Republic of Estonia, hereinafter referred to as the "Parties", desirous of laying down an arrangement on the mutual protection of classified information, have agreed as follows:

Article 1*Purpose and scope of application*

The purpose of this Agreement is to protect classified information transmitted between the Parties particularly for purposes of foreign affairs, defence, security, police or industrial matters, or transmitted for the preparation or implementation of classified contracts, or produced on the basis of or arising from transmitted classified information.

Article 2*Definitions*

For the purposes of this Agreement:

a) classified information means information or material transmitted or produced under this Agreement that is to be kept secret and has been marked with a classification marking under the national law of a Party so as to ensure that the information or material is appropriately protected;

b) contractor means an individual, a legal person or a public authority under the

de parts jurisdiktion och har behörighet att ingå kontrakt;

c) säkerhetsklassificerat kontrakt: ett kontrakt mellan två eller flera kontraktsparter, vilket för att kunna fullgöras kräver tillgång till eller användning av säkerhetsklassificerad information, eller där säkerhetsklassificerad information framställs för att fullgöra kontraktet eller uppkommer på grund av kontraktet;

d) nationell säkerhetsmyndighet: nationell myndighet som har ansvar för genomförandet och övervakningen av denna överenskommelse;

e) behörig myndighet: nationell säkerhetsmyndighet eller annan nationell myndighet som med stöd av den nationella lagstiftningen har ansvar för att genomföra denna överenskommelse;

f) utlämnande part: fördragsslutande part, från vilken den säkerhetsklassificerade informationen härrör;

g) mottagarpart: fördragsslutande part, till vilken den säkerhetsklassificerade informationen förmedlas;

h) nationell lagstiftning: lagar, författningar på lägre nivå samt myndighetsbestämmelser och -föreskrifter;

i) säkerhetsintyg baserat på en personsäkerhetsutredning: bedömning, utförd av behörig myndighet i enlighet med den nationella lagstiftningen, med vilken en person ges rätt att få tillgång till säkerhetsklassificerad information;

j) säkerhetsintyg baserat på en säkerhetsutredning som gäller sammanslutning: en handling, med vilken intygas att en juridisk person och dennas lokaler har vederbörlig fysisk och organisatorisk beredskap att använda och deponera säkerhetsklassificerad information i enlighet med relevant nationell lagstiftning;

k) informationsbehov: verifierat behov av säkerhetsklassificerad information.

jurisdiction of one of the Parties possessing the legal capacity to conclude contracts;

c) classified contract means a contract between two or more contractors the implementation of which requires access to, or the use of, classified information or where classified information is produced to implement the contract or arises from the contract;

d) National Security Authority means the national authority responsible for the implementation and supervision of this Agreement;

e) competent authority means the National Security Authority or other national authority which, under the national law, is responsible for the implementation of this Agreement;

f) originating Party means the Party initiating classified information;

g) recipient Party means the Party to which classified information is transmitted;

h) national law means laws, subordinate regulations, official instructions and guidelines;

i) personnel security clearance means a determination by the competent authority that allows a person to access classified information, in accordance with the relevant national law;

j) facility security clearance certificate means a document proving that a legal person and its facilities have the physical and organisational capability to use and deposit classified information, in accordance with the relevant national law;

k) need-to-know means a verified need to access classified information.

Artikel 3

Skydd av säkerhetsklassificerad information

1. De fördragsslutande parterna ska i enlighet med sin nationella lagstiftning vidta de åtgärder som fordras för att skydda säkerhetsklassificerad information. De ska ge sådan information samma skydd de ger egen information av motsvarande säkerhetsklass.

Article 3

Protection of classified information

1. The Parties shall take all appropriate measures under their national law to protect classified information. They shall afford such information the same protection as they afford to their own information at the corresponding level of classification.

2. De fördragsslutande parterna ska inte ge internationella organisationer eller stater som inte är parter i denna överenskommelse, medräknat deras tjänstemän, medborgare och juridiska personer, tillgång till säkerhetsklassificerad information, såvida inte den behöriga myndigheten hos den fördragsslutande part som har bestämt om klassificeringen på förhand har gett sitt skriftliga samtycke.

3. Säkerhetsklassificerad information får användas endast för det ändamål för vilket det har förmedlats.

4. Fysiska personer får ges tillgång till säkerhetsklassificerad information endast utgående från ett informationsbehov i deras arbete eller i utförandet av ett givet uppdrag.

5. Tillgång till information som har klassificerats som KONFIDENTIELL/KONFIDENTSIAALNE eller högre får endast ges fysiska personer som har ett säkerhetsintyg baserat på en personsäkerhetsutredning i enlighet med den nationella lagstiftningen.

6. De fördragsslutande parterna ska inom sina respektive territorier säkerställa att de säkerhetsgranskningar av lokaler och säkerhetsutredningar av fysiska personer som krävs för att genomföra denna överenskommelse sker på vederbörligt sätt.

Artikel 4

Säkerhetsklasserna

1. Säkerhetsklasserna motsvarar varandra enligt följande:

Republiken Finland
ERITTÄIN SALAINEN
SALAINEN
LUOTTAMUKSELLINEN
KÄYTTÖ RAJOITETTU

Republiken Estland
TÄIESTI SALAJANE
SALAJANE
KONFIDENTSIAALNE
PIIRATUD

2. Mottagarparten ska säkerställa att säkerhetsklassificerad information och kopior av sådan information förses med dess egen motsva-

2. The Parties shall not grant access to classified information to any international organisation or any state, including its officials, citizens and legal entities, that is not a Party to this Agreement, without the prior written consent of the competent authority of the Party which determined the classification.

3. Classified information shall be used solely for the purpose for which it has been transmitted.

4. Access to classified information may only be granted to individuals on account of their work or performance of a given task, on a need-to-know basis.

5. Access to information classified as LUOTTAMUKSELLINEN/KONFIDENTSIAALNE or above may only be granted to individuals who hold a personnel security clearance in accordance with the relevant national law.

6. In their respective territories, the Parties shall ensure that the security inspections of facilities and the background checks of individuals necessary for the implementation of this Agreement are appropriately carried out.

Article 4

Security Classification Levels

1. The security classifications levels shall correspond to one another as follows:

Republic of Finland
ERITTÄIN SALAINEN
SALAINEN
LUOTTAMUKSELLINEN
KÄYTTÖ RAJOITETTU

Republic of Estonia
TÄIESTI SALAJANE
SALAJANE
KONFIDENTSIAALNE
PIIRATUD

2. The recipient Party shall ensure that any classified information and any copies of such information are marked with a marking

rande nationella säkerhetsanteckning. Anteckning ska också göras på information som framställs utgående från förmedlad säkerhetsklassificerad information eller ett säkerhetsklassificerat kontrakt eller som uppkommer på denna grund.

3. Mottagarpartens nationella säkerhetsmyndighet ska säkerställa att säkerhetsklassen ändras eller hävs endast i det fall att den utlämnande partens nationella säkerhetsmyndighet ber om det eller ger sitt tillstånd till det.

4. Mottagarpartens nationella säkerhetsmyndighet kan be den utlämnande partens nationella säkerhetsmyndighet att ändra eller häva en säkerhetsklassificering eller att meddela grunderna för att man valt en viss säkerhetsklass.

designating the corresponding national security classification level. A marking shall be made also on information produced on the basis of or arising from transmitted classified information or a classified contract.

3. The National Security Authority of the recipient Party shall ensure that the security classification level is altered or revoked only when so requested or allowed by the National Security Authority of the originating Party.

4. The National Security Authority of the recipient Party may request the National Security Authority of the originating Party to alter the security classification level or revoke it, or to supply reasons for the choice of a given level of classification.

Artikel 5

Säkerhetsklassificerade kontrakt

1. Den utlämnande parten som ingår ett säkerhetsklassificerat kontrakt eller som tillåter att ett sådant kontrakt ingås med en kontraktspart som hör till mottagarpartens jurisdiktion ska av mottagarpartens behöriga myndighet erhålla ett säkerhetsintyg över kontraktsparten baserat på en säkerhetsutredning som gäller sammanslutning. Intyget måste erhållas innan en potentiell kontraktspart som deltar i ett anbudsförfarande ges tillgång till säkerhetsklassificerad information.

2. De behöriga myndigheterna ska säkerställa att säkerhetsklassificerade kontrakt både innehåller bestämmelser om kontraktspartens skyldighet att vidta nödvändiga åtgärder för att skydda säkerhetsklassificerad information och anvisningar om klassificering.

3. De behöriga myndigheterna ska säkerställa att säkerhetsklassificerade kontrakt innehåller bestämmelser om förbud att ingå säkerhetsklassificerade kontrakt med underleverantörer innan den behöriga myndigheten har gett sitt tillstånd. På underleverantörer tillämpas samma säkerhetskrav som på den kontraktspart som har ingått huvudkontraktet.

4. Mottagarpartens behöriga myndigheter ska säkerställa att säkerhetsklassificerade kontrakt genomförs på samma säkerhetsnivå som för säkerhetsklassificerade kontrakt som ingås av den fördragsslutande parten själv. För detta än-

Article 5

Classified contracts

1. The originating Party, which concludes, or permits the conclusion of, a classified contract with a contractor of the recipient Party, shall obtain from the competent authority of that Party a facility security clearance certificate based on a security vetting of the contractor. The certificate shall be obtained before access to classified information is granted to a potential contractor participating in a tender process.

2. The competent authorities shall ensure that classified contracts contain both provisions on the duty of the contractor to undertake the necessary measures for the protection of classified information and classification instructions.

3. The competent authorities shall ensure that classified contracts contain provisions that prohibit concluding a classified contract with a subcontractor before the competent authority has granted a permission to do so. Subcontractors shall be subject to the same security requirements as the contractor which concluded the main contract.

4. The competent authorities of the recipient Party shall ensure that the same standard of security is observed in the implementation of classified contracts as would be the case with classified contracts concluded by that Party

damål ska dessa behöriga myndigheter vidta följande åtgärder innan en kontraktspart ges tillgång till säkerhetsklassificerad information:

- a) säkerställa att kontraktsparten är förmögen att skydda säkerhetsklassificerad information på vederbörligt sätt;
- b) utfärda säkerhetsintyg baserade på person-säkerhetsutredningar till personer som har ett verifierat behov av tillgång till säkerhetsklassificerad information i sitt arbete eller för ett givet uppdrag;
- c) säkerställa att alla som har tillgång till säkerhetsklassificerad information är medvetna om sina skyldigheter i enlighet med tillämplig nationell lagstiftning;
- d) utföra säkerhetsgranskningar i de lokaler den övervakningsskyldighet gäller som avses i denna artikel.

itself. To this end, these competent authorities shall undertake the following measures before access to classified information is granted to the contractor:

- a) ensure that the contractor can offer appropriate protection to classified information;
- b) issue personnel security clearance certificates to those persons who have a verified need for access to classified information for reasons of work or performance of a given task;
- c) ensure that everyone with access to classified information is aware of his or her obligations under the applicable national law;
- d) carry out security inspections in facilities subject to the duty of supervision referred to in this Article.

Artikel 6

Förmedling av säkerhetsklassificerad information

1. Information som hör till säkerhetsklassen YTTERST HEMLIIG/TÄIESTI SALAJANE får förmedlas endast via officiella regeringskanaler.

2. Information som hör till säkerhetsklassen HEMLIIG/SALAJANE eller KONFIDENTIELL/KONFIDENTSIAALNE ska i normala fall förmedlas via officiella regeringskanaler. I brådskande fall eller i fråga om särskilt angivna projekt eller program kan även andra kanaler användas, förutsatt att bägge fördragsslutande parter nationella säkerhetsmyndigheter godkänner förfarandet.

3. Vid förmedling av information som hör till säkerhetsklassen KONFIDENTIELL/KONFIDENTSIAALNE eller högre ska följande krav iakttas:

- a) personen som transporterar handlingen eller materialet ska ha ett säkerhetsintyg baserat på en relevant personsäkerhetsutredning samt ett kuririntyg utställt av den behöriga säkerhetsmyndigheten;
- b) den utlämnande parten ska föra register över förmedlad säkerhetsklassificerad information och på begäran av mottagarparten ge den sistnämnda ett registerutdrag;

Article 6

Transmission of classified information

1. Information classified as ERITTÄIN SALAINEN/TÄIESTI SALAJANE shall only be transmitted through official Government-to-Government channels.

2. Normally, information classified as SALAINEN/SALAJANE or LUOTTAMUKSELLINEN/KONFIDENTSIAALNE shall be transmitted through official Government-to-Government channels. In urgent cases or for specific designated projects or programmes, other channels may also be used, subject to the approval of the National Security Authorities of both Parties.

3. The transmission of information classified as LUOTTAMUKSELLINEN/KONFIDENTSIAALNE and above shall meet the following requirements:

- a) the person carrying the document or material holds a security clearance certificate issued on the basis of an appropriate background check and a courier certificate issued by a competent authority;
- b) the originating Party maintains a register of transmitted classified information and, on request by the recipient Party, provides the latter with an extract of the register;

c) handlingarna och annat material som innehåller säkerhetsklassificerad information ska förpackas och förseglas på ett adekvat sätt;

d) mottagandet av säkerhetsklassificerad information ska bekräftas skriftligen.

4. Om man har för avsikt att förmedla en större mängd säkerhetsklassificerat material ska de nationella säkerhetsmyndigheterna från fall till fall komma överens om det lämpliga förfaringsättet.

5. Information som hör till säkerhetsklassen BEGRÄNSAD TILLGÅNG/PIIRATUD kan även förmedlas per post eller med någon annan leveransservice, med tillbörligt beaktande av den utlämnande partens nationella lagstiftning.

6. Säkerhetsklassificerad information får förmedlas elektroniskt endast fullt krypterat, med krypteringsmetoder och -apparater som bägge fördragsslutande parter behöriga myndigheter gemensamt har godkänt.

7. De fördragsslutande parternas säkerhetstjänster kan direkt sinsemellan utbyta operativ information eller underrättelseuppgifter i enlighet med nationell lagstiftning.

Artikel 7

Översättning, kopiering och utplåning av säkerhetsklassificerad information

1. Information som hör till säkerhetsklassen YTTERST HEMLIG/TÄIESTI SALAJANE eller HEMLIG/SALAJANE får översättas eller kopieras endast om den utlämnande partens nationella säkerhetsmyndighet på förhand har gett sitt skriftliga samtycke.

2. Information som hör till säkerhetsklassen HEMLIG/SALAJANE eller KONFIDENTIELL/KONFIDENTSIAALNE ska returneras till den utlämnande parten eller utplånas i enlighet med den nationella lagstiftningen.

3. Information som hör till säkerhetsklassen YTTERST HEMLIG/TÄIESTI SALAJANE ska, när det anses att den inte längre behövs, returneras till den utlämnande parten iakttagande förfarandet som föreskrivs i artikel 6 och beaktande mottagarpartens lagstiftning.

4. I krissituationer, där säkerhetsklassificerad information som har framställts eller överförts i enlighet med denna överenskommelse inte kan skyddas eller returneras, ska den säkerhetsklas-

c) the documents and other materials containing classified information are appropriately packaged and sealed;

d) the receipt of classified information is confirmed in writing.

4. If a large volume of classified information is to be transmitted, the applicable procedures shall be agreed upon by the National Security Authorities on a case-by-case basis.

5. Information classified as KÄYTTÖ RAJOITETTU/PIIRATUD may also be transmitted by post or another delivery service, taking due note of the requirements of the national law of the originating Party.

6. Classified information may be transmitted electronically only in a fully encrypted mode, using encryption methods and devices jointly approved by the competent authorities of both Parties.

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

Article 7

Translation, copying and disposal of classified information

1. Information classified as ERITTÄIN SALAINEN/TÄIESTI SALAJANE or SALAINEN/SALAJANE may be translated or copied if the National Security Authority of the originating Party has given a prior written consent for it.

2. Information classified as SALAINEN/SALAJANE or LUOTTAMUKSELLINEN/KONFIDENTSIAALNE shall be returned to the originating Party or disposed of in accordance with national law.

3. Information classified as ERITTÄIN SALAINEN/TÄIESTI SALAJANE shall be returned to the originating Party in accordance with the procedure provided in Article 6 after it is no longer considered necessary, taking into account the national law of the recipient Party.

4. In case of a crisis situation which makes it impossible to protect and return classified information generated or transmitted according to this Agreement, the classified information

sificerade informationen omedelbart förstöras. Mottagarparten ska så fort som möjligt underätta den utlämnande partens nationella säkerhetsmyndighet om att säkerhetsklassificerad information har förstörts.

shall be destroyed immediately. The recipient Party shall notify the National Security Authority of the originating Party about the destruction of classified information as soon as possible.

Artikel 8

Besök

1. En fördragsslutande part ska tillåta besök från den andra fördragsslutande parten för säkerhetsgranskningar i lokaler där säkerhetsklassificerad information framställs, hanteras eller förvaras, eller där det drivs säkerhetsklassificerade projekt, endast om mottagarpartens behöriga myndighet på förhand har gett sitt skriftliga tillstånd. Ett sådant tillstånd ska endast beviljas personer som har ett säkerhetsintyg baserat på en personsäkerhetsutredning och ett informationsbehov.

2. Vardera fördragsslutande parten ska tillåta att myndighetspersonal eller anställda hos en kontraktspart från den andra fördragsslutande parten besöker sådana egna eller en kontraktsparts lokaler där besökare kan få tillgång till säkerhetsklassificerad information. Besökare ska uppfylla kraven i artikel 3.4 och 3.5.

3. Besökare ska följa de nationella säkerhetsbestämmelser och -föreskrifter som tillämpas hos värdorganisationen och i dess lokaler. Säkerhetsklassificerad information som har överlåtit till besökare ska anses ha överlåtit till den fördragsslutande part, vars myndigheter besökarna företräder, eller till vars jurisdiktion den kontraktspart hör som besökarna representerar eller som är deras arbetsgivare, och den överlåtna informationen ska skyddas i enlighet med det.

4. Om man under ett besök vill få tillgång till information som hör till säkerhetsklassen KONFIDENTIELL/KONFIDENTSIAALNE eller högre måste besöksansökan tillställas mottagarparten via officiella regeringskanaler. Förfarandet med besöksansökningar ska begränsas till besök som gäller företagssäkerhet eller säkerhetsgranskningar.

5. Besöksansökan ska framföras minst två (2) veckor före den planerade tidpunkten för besöket på mottagarpartens nationella språk eller på engelska. Besöksansökan ska innehålla de

Article 8

Visits

1. Security inspection visits to premises where classified information is developed, handled or stored, or where classified projects are carried out, shall only be granted by one Party to visitors from the other Party if a prior written permission from the Competent Authority of the recipient Party has been obtained. Such permission shall only be granted to persons who have a personnel security clearance and a need-to-know.

2. Each Party shall allow visits by personnel of the administration or of a contractor of the other Party to its own or its contractor's facilities, where the visitors may have access to classified information. The visitors shall meet the requirements referred to in paragraphs 4 and 5 of Article 3.

3. The visitors shall abide by the national security instructions and guidelines applicable in the host agency and its facility. Classified information that has been provided to the visitors shall be deemed to have been provided to the Party whose administration the visitors represent or which exercises jurisdiction over the contractor whom the visitors represent or are employed by; the information shall be secured accordingly.

4. If, during a visit, information classified as LUOTTAMUKSELLINEN/KONFIDENTSIAALNE or above is to be accessed, the visit request shall be submitted to the host Party solely through official Government-to-Government channels. The visit request procedure shall be limited only to industrial security visits and security inspection visits.

5. The visit request shall be submitted at least two (2) weeks before the intended time of the visit, either in the national language of the host Party or in English. The visit request shall

uppgifter som anges i bilagan till denna överenskommelse.

6. I enlighet med kriterier som de behöriga myndigheterna sinsemellan har avtalat om kan de fördragsslutande parterna göra upp förteckningar över personal som har rätt till flera än ett besök i anslutning till ett enskilt projekt, program eller upphandlingsavtal. Dessa förteckningar ska gälla i tolv (12) månader. Förteckningarnas giltighetstid kan emellertid genom ett avtal mellan de fördragsslutande parterna förlängas med högst tolv (12) månader åt gången.

7. Avtal om förteckningar ska ingås och förteckningar göras upp i enlighet med mottagartens nationella lagstiftning. När en förteckning har gjorts upp kan detaljerna kring ett enskilt besök avtalas direkt med den kontraktspart eller organisation som ska besökas.

contain the information referred to in the Annex to this Agreement.

6. In accordance with conditions agreed upon by their competent authorities, the Parties may draw up lists of personnel who are entitled to more than one visit in the context of an individual project, programme or procurement contract. Such lists shall have a period of validity of twelve (12) months. However, the period of validity of such lists may be extended, by agreement between the Parties, for at most twelve (12) months at a time.

7. The agreement on the lists shall be concluded and the lists shall be drawn up in accordance with the national law of the host Party. Once a list has been drawn up, the particulars of a single visit may be agreed upon directly with the contractor or agency to be visited.

Artikel 9

Underrättelser och samråd

1. De fördragsslutande parterna ska främja samarbetet mellan de behöriga myndigheterna och för att genomföra denna överenskommelse underrätta varandra om följande:

a) den nationella lagstiftningen om skydd av säkerhetsklassificerad information och sådana ändringar i den som kan påverka skyddet av säkerhetsklassificerad information som utbyts i enlighet med denna överenskommelse, som uppkommer till följd av den eller som framställs utgående från den;

b) nationella säkerhetsmyndigheter och ändringar som gäller dem.

2. För att säkerställa ett nära samarbete i genomförandet av denna överenskommelse ska de nationella säkerhetsmyndigheterna samråda sinsemellan på någondera myndighetens begäran.

Artikel 10

Tvistlösning

Alla tvister som uppkommer mellan de fördragsslutande parterna om tolkning eller tillämpning av denna överenskommelse ska avgöras endast och enbart i samråd mellan parterna.

Article 9

Notification and consultations

1. The Parties shall promote the co-operation between their competent authorities and, in order to implement this Agreement, notify each other of the following:

a) national laws on the protection of classified information and amendments to such laws, when these may affect the protection of classified information to be exchanged, arising or produced under this Agreement;

b) the designation of National Security Authorities and any changes thereto.

2. In order to ensure close co-operation in the implementation of this Agreement, the National Security Authorities of the Parties shall consult each other at the request of one of these authorities.

Article 10

Resolution of disputes

All disputes between the Parties on the interpretation or application of this Agreement shall be resolved exclusively by means of consultations between the Parties.

Artikel 11

Kränkningar av sekretessbestämmelserna för säkerhetsklassificerad information

1. Vardera fördragsslutande parten ska omedelbart underrätta den andra fördragsslutande parten om misstänkta eller upptäckta fall av obehörigt röjande av säkerhetsklassificerad information som avses i denna överenskommelse eller av andra kränkningar av sekretessen för sådan information.

2. Den fördragsslutande part till vars jurisdiktion ärendet hör ska i enlighet med sin nationella lagstiftning vidta alla åtgärder som fordras för att begränsa konsekvenserna av sådana kränkningar som avses i punkt 1 i denna artikel och för att förhindra att kränkningarna fortgår. Den andra fördragsslutande parten ska på begäran bistå undersökningarna och underrättas om undersökningarnas resultat och om vilka åtgärder som vidtagits till följd av kränkningen.

Artikel 12

Kostnader

De fördragsslutande parterna ersätter inte varandra för kostnader som förorsakas av genomförandet av denna överenskommelse.

Artikel 13

Slutbestämmelser

1. De fördragsslutande parterna ska underrätta varandra om att de åtgärder som den nationella lagstiftningen kräver för att sätta denna överenskommelse i kraft har uppfyllts. Överenskommelsen träder i kraft den första dagen den andra månaden efter att den senare underrättelsen har tagits emot.

2. Denna överenskommelse ska gälla tills vidare. Överenskommelsen kan ändras med ömsesidigt skriftligt samtycke av de fördragsslutande parterna. Vardera fördragsslutande parten kan när som helst föreslå ändringar i överenskommelsen. Om en fördragsslutande part så föreslår, ska de fördragsslutande parterna inleda förhandlingar om ändringar i överenskommelsen.

Article 11

Violations of provisions on the protection of classified information

1. Each Party shall immediately notify the other Party of any suspicions or discoveries of unlawful disclosure of classified information referred to in this Agreement or of other violations of the protection of such information.

2. The Party with jurisdiction shall undertake all possible appropriate measures under its national law so as to limit the consequences of violations referred to in paragraph 1 of this Article and to prevent further violations. Upon request, the other Party shall provide investigative assistance; it shall be informed of the outcome of the investigation and of the measures undertaken as a result of the violation.

Article 12

Costs

The Parties shall not reimburse each other for the costs incurred in the implementation of this Agreement.

Article 13

Final provisions

1. The Parties shall notify each other of the completion of the national procedures necessary for the entry into force of the Agreement. The Agreement shall enter into force on the first day of the second month following the receipt of the later notification.

2. This Agreement shall be in force for an indeterminate period of time. The Agreement may be amended by the mutual, written consent of the Parties. Either Party may propose amendments to this Agreement at any time. If one Party so proposes, the Parties shall begin consultations on the amendment of the Agreement.

3. En fördragsslutande part kan säga upp denna överenskommelse genom att skriftligt via regeringskanaler underrätta den andra fördragsslutande parten om uppsägningen, med iakttagande av en sex (6) månaders uppsägningstid. Om överenskommelsen sägs upp ska redan förmedlad säkerhetsklassificerad information och klassificerad information som uppkommer på grund av denna överenskommelse hanteras i enlighet med bestämmelserna i denna överenskommelse så länge det är nödvändigt för att skydda den säkerhetsklassificerade informationen.

Till bekräftelse härav har i vederbörlig ordning befullmäktigade representanter för de fördragsslutande parterna undertecknat denna överenskommelse

i Tallinn den 5 juni 2007

i två original, båda på finska, estniska och engelska språken, vilka alla texter är lika giltiga. I fall av skiljaktighet i fråga om tolkningen ska den engelska texten ha företräde.

3. A Party may terminate this Agreement by written notification to the other Party delivered through official Government-to-Government channels, observing a period of notice of six (6) months. If the Agreement is terminated, the classified information already transmitted and the classified information arising from this Agreement shall be handled in accordance with the provisions of this Agreement for as long as necessary for the protection of the classified information.

In witness whereof, the duly authorised representatives of the Parties have signed this Agreement,

in Tallinn on the 5th day of June, 2007

in two originals, both in the Finnish, Estonian, and English languages, each text being equally authentic. In case of any divergence of interpretation the English text shall prevail.

För republiken Finlands regering

For the Government of the Republic of
Finland

För republiken Estlands regering

For the Government of the Republic of
Estonia

Bilaga*Besöksansökan*

Alla besöksansökningar som avses i artikel 8 i överenskommelsen ska innehålla följande uppgifter:

1. besökarens förnamn och efternamn, födelsedatum och födelseort samt passnummer eller identitetsbevisets nummer;
2. besökarens nationalitet;
3. besökarens tjänsteställning eller uppdrag samt namnet på den myndighet, organisation eller de lokaler, till vars personal besökaren hör;
4. besökarens säkerhetsintyg baserat på en personsäkerhetsutredning som innehåller uppgifter om omfattningen på personens befogenheter att få tillgång till säkerhetsklassificerad information;
5. syftet med besöket och den föreslagna tidpunkten för besöket;
6. organisationerna och lokalerna som ska besökas samt namnen på deras kontaktpersoner.

Annex*Visit requests*

All visit requests referred to in Article 8 of the Agreement shall contain the following information:

1. the given name and surname of the visitor, his or her date and place of birth, and the number of his or her passport or identity card;
2. the citizenship of the visitor;
3. the position or service designation of the visitor, as well as the name of the authority, agency or facility to whose personnel the visitor belongs;
4. the grade of the security clearance of the visitor, indicating the scope of his or her right to access classified information;
5. the purpose of the visit and its proposed date;
6. the agencies and facilities to be visited and the contact persons there.