RP 283/2014 rd

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

PROPOSITIONENS HUVUDSAKLIGA INNEHÅLL

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

Syftet med överenskommelsen är att säkerställa skyddet av sekretessbelagd säkerhetsklassificerad information mellan Finland och Kroatien i samarbetet mellan parterna särskilt i utrikes-, försvars-, säkerhets- och polisfrågor samt i vetenskaps-, näringslivs- och teknologifrågor. Det är fråga om känsligt informationsmaterial som särskilt har klassificerats på en hög informationssäkerhetsnivå i den utlämnande fördragsslutande staten. Överenskommelsen förpliktar inte till utbyte av säkerhetsklassificerad information.

Överenskommelsen träder i kraft den första dagen i den andra månaden efter att den senare underrättelsen har mottagits där parterna meddelar varandra att de nationella åtgärderna har slutförts som ikraftträdandet av överenskommelsen förutsätter. 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 statsrådet.

297430

INNEHÅLL

ALLMÄN MOTIVERING

1 Inledning

Med informationssäkerhet avses alla förfaranden som skyddar informationsinnehållet gentemot utomstående (informationens konfidentialitet), informationens oföränderlighet (informationens integritet) samt informationens användbarhet. För att trygga informationssäkerheten används olika metoder. De vanligaste är kontroll av personalens tillförlitlighet och verksamhetsutrymmenas säkerhet, sekretessbestämmelser och begränsningar i rätten att använda informationen enbart för angivet ändamål, samt olika typer av procedurkrav för hantering och överföring av information. Informationssäkerhetskraven täcker informationens hela livscykel, inbegripet förvärvande, bearbetning, användning, överlåtelse, arkivering och utplåning.

Inom det internationella samarbetet förekommer det stundom 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 hanteras särskilt omsorgsfullt. Det gäller Finlands trovärdighet som part i det internationella samarbetet. Det internationella informationssäkerhetssamarbetet, som även Finland är delaktig i, omfattar sedvanligt skydd av icke-offentligt informationsutbyte som ingår i den diplomatiska verksamheten, liksom även i samarbetet mellan försvarsförvaltningarna. 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 säkerhetsklassificerad information. Det här gäller särskilt då det är fråga om myndighetsupphandling som förutsätter att sekretessbelagd statlig information ges ut till ett företag för att ett kommersiellt kontrakt ska kunna genomföras. Traditionellt hör anskaffningar av detta slag särskilt till försvarets område, men nuförtiden i allt högre grad också anskaffningar inom andra sektorer, såsom informationsteknologi och kärnkraft.

Det har trots olika strävanden inte visat sig vara möjligt att få till stånd en multilateral konvention inom området för informationssäkerhet. Den största orsaken är skillnaderna i nationell lagstiftning samt i administrativa strukturer och kutymer, vilket återspeglar känsligheten i informationssäkerhetsfrågor som en del av den nationella säkerheten överlag. Ett undantag från detta är det generella säkerhetsskyddsavtalet om ömsesidigt skydd och utbyte av säkerhetsskyddsklassificerade uppgifter mellan Danmark, Finland, Island, Norge och Sverige (FördrS 11 och 12/2013).

Bristen på en konvention har tvingat staterna, Finland medräknat, att lösa frågan genom bilaterala avtal. Finland ingick sitt första bilaterala avtal om informationssäkerhet med Tyska förbundsrepubliken år 2004. Avtalet trädde i kraft den 16 juli 2004 (FördrS 96 och 97/2004). Ett år senare undertecknades ett avtal mellan Finland och Frankrike och det trädde i sin tur i kraft den 1 augusti 2005 (FördrS 66 och 67/2005). Dessa båda stora medlemmar av Europeiska unionen 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 kallad ESA-överenskommelsen, även den från 2004 (FördrS 94 och 95/2004). En av de viktigaste målsättningarna med överenskommelsen har varit att säkerställa det finska näringslivets möjligheter att på jämlik grund med de andra medlemsländerna kunna delta i ESA:s säkerhetsklassificerade anbudsförfaranden. Fin-

land har också ingått ett säkerhetsskyddsavtal med Västeuropeiska unionen VEU (FördrS 41 och 42/1998), med Organisationen för gemensamt försvarsmaterielsamarbete i Europa OCCAR (FördrS 109 och 110/2008) och med Nordatlantiska fördragsorganisationen Nato (FördrS 7 och 8/2013). Utöver dessa fördrag har Finland gällande överenskommelser om informationssäkerhet med Slovakien (FördrS 116 och 117/2007), Estland (FördrS 12 och 13/2008), Italien (FördrS 23 och 24/2008), Lettland (FördrS 33 och 34/2008), Polen (FördrS 46 och 47/2008), Bulgarien (FördrS 116 och 117/2008), Slovenien (FördrS 22 och 23/2009), Tjeckien (FördrS 53 och 54/2009), Spanien (FördrS 22 och 23/2010), Amerikas förenta stater (FördrS 41 och 42/2013), Storbritannien (FördrS 49 och 50/2013), Luxemburg (FördrS 59 och 60/2013) och Schweiz (FördrS 88 och 89/2014). Den 10 maj 2012 godkände Finland det i maj 2011 undertecknade avtalet mellan EU:s medlemsstater om skydd av säkerhetsskyddsklassificerade uppgifter. Ytterligare har Finland ingått en snävare överenskommelse med Israel om säkerhetsklassificerad information som förmedlas mellan försvars- och säkerhetsförvaltningarna (FördrS 34 och 35/2012).

Med överenskommelser om informationssäkerhet skapas förutsättningar för utbyte av säkerhetsklassificerad information mellan parterna. Genom överenskommelser säkerställs att säkerhetsklassificerad information som Finland lämnar ut hålls hemlig i mottagarstaten och skyddas och hanteras på ett korrekt sätt. Tack vare en informationssäkerhetsöverenskommelse kan också den andra parten försäkra sig om att Finland på ett korrekt sätt skyddar och hanterar säkerhetsklassificerad information som den lämnar ut.

2 Nuläge

2.1 Lagen 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 samt ESA-överenskommelsen sattes i kraft. Lagen ansågs nödvändig, bland annat för att genomförandet av internationella överenskommelser tvingar till avvikelser från våra nationella regleringar om handlingars offentlighet och säkerhet, med huvudsaklig grund i lagen om offentlighet i myndigheternas verksamhet (621/1999), nedan kallad 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 finsk myndighet och den utlämnande parten, i enlighet med en internationell överenskommelse som är bindande för Finland eller med någon annan internationell förpliktelse, har försett försändelsen med en anteckning om säkerhetsklass. Bestämmanderätten till utlämnad information kvarstår hos den utlämnande staten även efter att den utlämnats. Lagen kan endast tillämpas om den internationella överenskommelsen har satts i kraft i Finland på det sätt som grundlagen kräver eller om det är fråga om en internationell förpliktelse som annars är bindande för Finland.

Till kategorin särskilt känsligt informationsmaterial som omfattas av lagens tillämpningsområde hänförs dessutom handlingar som har upprättats av en finsk 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 särskilt känsligt informationsmaterial. Lagen tillämpas inte endast för hemlighållande eller klassificering av handlingar och delar av handlingar som innehåller nationell information som Finland

Lagens tillämpningsområde

förpliktelser 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.

Pågående ändringar

En ny säkerhetsutredningslag (726/2014) träder i kraft den 1 januari 2015. Lagen upphäver lagen om säkerhetsutredningar (177/2002). Samtidigt ändras i lagen om internationella förpliktelser som gäller informationssäkerhet 11 § om säkerhetsutredning av person, 12 § om säkerhetsutredningar som gäller sammanslutningar och 14 § om intyg över säkerhetsutredningar (Lag om ändring av lagen om internationella förpliktelser som gäller informationssäkerhet, 731/2014). Till lagen om internationella förpliktelser som gäller informationssäkerhet fogas en ny 20 a § om ändringssökande och 13 § om en förbindelse om att vidta säkerhetsåtgärder upphävs, men motsvarande bestämmelse inkluderas i säkerhetsutredningslagen (40 §). Även ändringarna till lagen om internationella förpliktelser som gäller informationssäkerhet träder i kraft den 1 januari 2015.

Lagens förhållande till offentlighetslagstiftningen

Lagen om internationella förpliktelser som gäller informationssäkerhet innehåller bestämmelser som avviker från bestämmelserna om informationssäkerhet för nationella handlingar. I lagen ingår emellertid en allmän hänvisning till offentlighetslagen. Till de delar finska myndigheters handlingar innehåller annan information om internationellt samarbete än sådan som omfattas av internationella förpliktelser om informationssäkerhet ska offentlighetslagen och med stöd av den utfärdade bestämmelser tillämpas. Lagen innehåller dessutom en specialbestämmelse om beslutanderätten i situationer där det med stöd av offentlighetslagen frågas efter information om särskilt känsligt material. Enligt offentlighetslagen kan en begäran om information behandlas och avgöras av den myndighet som förfogar över handlingen. En begäran om att få ta del av en handling kan dock överföras till en annan myndighet för beslut i de 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 kontrakt eller deltar i ett upphandlingsförfarande innan ett sådant kontrakt ingås 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 verkställande av ett kontrakt kan förutsätta tillgång till särskilt känsligt informationsmaterial (2 § 3 punkten).

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 kan en näringsidkare begära att det görs en säkerhetsutredning och en bedömning som gäller sammanslutningar (12 § 2 mom.). Motsvarande bestämmelse ingår i den nya säkerhetsutredningslagen (33 §:n 2 mom.). Syftet med bestämmelsen är att säkerställa finska 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 §). För att uppfylla internationella förpliktelser som gäller informationssäkerhet är en näringsidkare också skyldig att lämna behöriga säkerhetsmyndigheter information samt låta representanter för myndigheter, internationella organ

och fördragsslutande stater bekanta sig med sina säkerhetsarrangemang och verksamhetsutrymmen (16 § 2 mom. och 18 § 2 mom.).

Verkställande myndigheter

I lagen finns det bestämmelser (4 §) om de myndigheter som ska sköta internationella förpliktelser som gäller informationssäkerhet. Utrikesministeriet är Finlands nationella säkerhetsmyndighet *(National Security Authority, NSA)* i uppfyllandet av internationella förpliktelser som gäller informationssäkerhet. Försvarsministeriet, huvudstaben, Skyddspolisen och Kommunikationsverket är utsedda säkerhetsmyndigheter *(Designated Security Authority, DSA)*. I dessa myndigheters uppgifter kan bland annat ingå säkerhetsklassificering av handlingar som anknyter till anbuds- och upphandlingsförfaranden.

Skyddspolisen och huvudstaben svarar för utredningar som gäller personsäkerhet (11 §), säkerhetsutredning av person. Enligt lagen hör säkerhetsutredningar som gäller sammanslutningar till Skyddspolisen, utom då det är fråga om anskaffningar som hänför sig till försvaret, då utredningen görs av huvudstaben (12 §). Motsvarande bestämmelse om myndigheternas behörighet ingår i den nya säkerhetsutredningslagen (9 §). När de redogjorda ändringarna i lagen om internationella förpliktelser som gäller informationssäkerhet har trätt i kraft görs säkerhetsutredning av person och säkerhetsutredning av företag som förutsätts i en internationell förpliktelse som gäller informationssäkerhetsförpliktelse så som föreskrivs i den nya säkerhetsutredningslagen. Intyg över säkerhetsutredning av person eller av företag ger då den nationella säkerhetsmyndigheten, om inte något annat följer av särskilda skäl (ändrade 11 och 12 §).

Enligt 5 § 2 mom. i lagen om internationella förpliktelser som gäller informationssäkerhet kan den nationella säkerhetsmyndigheten och de utsedda säkerhetsmyndigheterna, oavsett vad som föreskrivs om behörighet att göra säkerhetsutredningar som gäller sammanslutningar, avtala om att sköta en viss uppgift eller ett visst uppgiftsområde för den andra säkerhetsmyndighetens räkning, om ett sådant arrangemang behövs för att uppgifterna ska kunna skötas på ett ändamålsenligt, ekonomiskt och flexibelt sätt. I 4 § 1 mom. i den lagen (885/2010) utses Kommunikationsverket till säkerhetsmyndighet med uppgift att fungera som sakkunnig i fråga om säkerheten hos informationssystem och telekommunikation.

I lagen om internationella förpliktelser som gäller informationssäkerhet finns det bestämmelser om myndigheters och näringsidkares informationsskyldighet (16 §). Syftet med bestämmelserna är att säkerställa att behöriga säkerhetsmyndigheter får den information de behöver för att sköta sina uppgifter. För samarbete som är baserat på en internationell förpliktelse om informationssäkerhet får myndigheterna, oavsett sekretessbestämmelser, också lämna ut sekretessbelagd information till den utländska fördragsslutande parten (17 §). Vidare har en myndighet rätt att inom ramen för en internationell förpliktelse om informationssäkerhet låta representanter för internationella organisationer och organ samt för fördragsslutande stater bekanta sig med sina säkerhetsarrangemang och verksamhetsutrymmen, oberoende av vad som föreskrivs om sekretessbeläggning av säkerhetsarrangemangen eller vad som föreskrivs eller bestäms om tillträde till utrymmen där sekretessbelagd information hanteras eller förvaras (18 §).

Den nationella säkerhetsmyndigheten ska enligt lagen i sådana fall som avses i en internationell förpliktelse som gäller informationssäkerhet underrätta den andra fördragsslutande parten, om sådant äventyrande av skyddet för säkerhetsklassificerad information och om sådant överträdande av en bestämmelse om informationssäkerhet som myndigheten fått kännedom om, samt vidta åtgärder för att utreda ärendet och för att väcka åtal mot den som gjord sig skyldig till en straffbar gärning. (19 §).

Sekretessbeläggning och reglering av informationsanvändningen

Särskilt känsligt informationsmaterial ska sekretessbeläggas, om inte annat följer av en internationell förpliktelse som gäller infor-

mationssäkerhet (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. I enlighet med den bestämmelsen får särskilt känsligt informationsmaterial användas och överlåtas endast för angivet ändamål, om inte den som har klassificerat materialet samtycker till något annat. Användningen av särskilt känsligt informationsmaterial är alltså 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 (8 §). Ju högre materialets säkerhetsklass är, desto strängare säkerhetsåtgärder krävs det. 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 säkerhetsåtgärder som motsvarar de olika säkerhetsklasserna vid hantering av särskilt känsligt informationsmaterial (9 §). I 11 § i statsrådets förordning om informationssäkerheten inom statsförvaltningen (681/2010), nedan kallad informationssäkerhetsförordningen, finns det särskilda bestämmelser om anteckningen om säkerhetsklassificering och i 12 § om säkerhetsklassificeringens motsvarighet.

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

Myndigheterna ska vara restriktiva i användningen av säkerhetsklassificerad information och därför har det allmänna kravet som finns i internationella överenskommelser på att endast personer som behöver informationen för skötseln av sina uppgifter ska ges tillgång till den skrivits in i lagen om internationella förpliktelser som gäller informationssäkerhet. Dessa personer ska namnges på förhand, om det förutsätts i överenskommelsen. Detsamma gäller näringsidkare som avses i 1 § 2 mom. (6 § 3 mom.).

Personalsäkerhet

Säkerhetsutredningar av person som förutsätts i internationella förpliktelser om informationssäkerhet ska göras så som föreskrivs i och med stöd av lagen om säkerhetsutredningar (177/2002). När ändringarna i lagen om internationella förpliktelser som gäller informationssäkerhet har trätt i kraft görs säkerhetsutredning av person som förutsätts i en internationell förpliktelse som gäller informationssäkerhet så som föreskrivs i den nya säkerhetsutredningslagen. Till exempel den personens rättigheter som är föremål för utredningen fastställs alltså enligt den lagen.

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 ska innehålla någon bedömning av en persons tillförlitlighet nämns bedömningen av en persons tillförlitlighet särskilt i lagen om internationella förpliktelser som gäller informationssäkerhet. En sådan bedömning ska på basis av säkerhetsutredningen göras av den nationella säkerhetsmyndigheten eller, om så har överenskommits mellan säkerhetsmyndigheterna, av den för uppgiften utsedda säkerhetsmyndigheten (11 § 3 mom.). Utgående från bedömningen utfärdas ett personsäkerhetsintyg (Personnel Security Clearance Certificate). Intyget skickas vanligtvis till fördragspartens säkerhetsmyndighet på det sätt som anges i överenskommelsen. I lagen föreskrivs det också om överlåtande av intyget till den berörda personen själv (14 §).

Inte heller enligt den nya säkerhetsutredningslagen får ett intyg över säkerhetsutredning av person innehålla myndighetens bedömning av hans eller hennes oförvitlighet, tillförlitlighet eller lämplighet för en tjänst eller ett uppdrag (42 §). Enligt 43 § utfärdar den nationella säkerhetsmyndigheten i enlighet med lagen om internationella förpliktelser som gäller informationssäkerhet sådana intyg över säkerhetsutredning av person som behövs för att uppfylla internationella förpliktelser som gäller informationssäkerhet. När ändringen av lagen om internationella förpliktelser som gäller informationssäkerhet har trätt i kraft ska den myndighet som gjort utredningen för utfärdandet av intyg och prövningen i anslutning till detta trots sekretessbestämmelserna lämna den nationella säkerhetsmyndigheten information om alla sådana omständigheter som vid utredningen framkommit i fråga om den som utredningen gäller (ändrade 11 § 1 mom.). På bedömningen av huruvida ett intyg ska utfärdas, på intygets giltighetstid och på återkallelse tillämpas säkerhetsutredningslagen (ändrade 11 § 2 mom.).

Säkerhetsutredning som gäller sammanslutning

Bestämmelser om säkerhetsutredningar och bedömningar som gäller sammanslutningar finns i 12 § i lagen om internationella förpliktelser som gäller informationssäkerhet. Säkerhetsutredningar som gäller sammanslutningar ska dels säkerställa att verksamhetsutrymmen och hanteringskutymer 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 verksamhetsutrymmen, och nödvändiga åtgärder vidtas med hjälp av ett avtal som ingås med näringsidkaren. Utredningen görs av Skyddspolisen. När det gäller försvarsanskaffningar är det dock huvudstaben som gör utredningen. Vid utredningen ska 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. Som ett led i en säkerhetsutredning som gäller en sammanslutning utreder och bedömer Kommunikationsverket vid behov huruvida en näringsidkares informationssystem och telekommunikation uppfyller de krav som följer av internationella förpliktelser som gäller informationssäkerhet.

De utsedda säkerhetsmyndigheterna kan vid säkerhetsutredningar som gäller sammanslutningar inom deras verksamhetsområde samt bedömningar som görs utgående från säkerhetsutredningarna enligt 13 § i lagen förutsätta att näringsidkaren förbinder sig att vidta de åtgärder som avses i 12 § 1 mom. och andra åtgärder som behövs för att uppfylla internationella förpliktelser som gäller informationssäkerhet. I förbindelsen kan man närmare precisera de åtgärder som näringsidkaren ska vidta för att uppfylla kraven som följer av internationella informationssäkerhetsförpliktelser. I den förbinder sig näringsidkaren också att justera sin verksamhet i enlighet med säkerhetskartläggningen. Efter att en säkerhetsutredning och en eventuell förbindelse har gjorts kan Skyddspolisen eller huvudstaben göra en bedömning av näringsidkarens tillförlitlighet och utfärda ett säkerhetsintyg (Facility Security Clearance Certificate).

När ändringarna i lagen om internationella förpliktelser som gäller informationssäkerhet har trätt i kraft görs säkerhetsutredning av företag som förutsätts i en internationell förpliktelse som gäller informationssäkerhet så som föreskrivs i den nya säkerhetsutredningslagen. Intyget över säkerhetsutredning av företag utfärdas dock av den nationella säkerhetsmyndigheten, om inte något annat följer av särskilda skäl. Den myndighet som gjort utredning ska för utfärdandet av intyg och prövningen i anslutning till detta trots

sekretessbestämmelserna lämna den nationella säkerhetsmyndigheten information om alla sådana omständigheter som vid utredningen framkommit i fråga om den som utredningen gäller (ändrade 12 § 1 mom.). På intygets giltighetstid och återkallelse tillämpas säkerhetsutredningslagen (ändrade 12 § 2 mom.).

2.2 Lagstiftningen om säkerhetsutredningar

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

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

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

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

Syftet med den nya säkerhetsutredningslagen som träder i kraft i januari 2015 är att främja möjligheterna att förebygga verksamhet som kan medföra skada för statens säkerhet, försvaret, Finlands internationella förbindelser, den allmänna säkerheten eller något annat med dessa jämförbart allmänt intresse eller enskilda ekonomiska intressen av synnerligen stor betydelse. Den nya lagen innefattar bestämmelser bl.a. om ställning och rättigheter för den som utredningen gäller (2 kap.), behöriga myndigheter och styrning av deras prövningsrätt (3 kap.), säkerhetsutredning av person (4 kap.), säkerhetsutredning av företag (5 kap.), avslutande av ett förfarande med säkerhetsutredning (6 kap.), registret över säkerhetsutredningar (7 kap.) samt giltigheten av säkerhetsutredningar och intyg över säkerhetsutredning (8 kap.).

Enligt den nya säkerhetsutredningslagen har Skyddspolisen allmän behörighet att besluta om huruvida en säkerhetsutredning ska göras (9 § 1 mom.). Huvudstaben gör säkerhetsutredningen, om den som utredningen gäller arbetar eller kommer att arbeta inom försvarsmakten eller sköter ett uppdrag på förordnande av försvarsmakten eller om säkerhetsutredningen hänför sig till verksamhet eller upphandling inom försvarsmakten. Huvudstaben gör säkerhetsutredningen av ett företag som sköter eller kommer att sköta ett uppdrag på förordnande av försvarsmakten eller av ett företag som hänför sig till upphandling inom försvarsmakten (9 § 3 mom.). Kommunikationsverket gör som ett led i en säkerhetsutredning av företag en utredning om nivån på informationssäkerheten i informationssystem och datakommunikation (9 § 4 mom.).

Också enligt den nya säkerhetsutredningslagen är säkerhetsutredningar av person mycket formbundna och kan genomföras endast med skriftligt samtycke på förhand av den som utredningen gäller (5 §). En utredning kan vara begränsad, normal eller omfattande (14 §). I 15 § bestäms om rätten att ansöka om säkerhetsutredning av person. Informationskällorna för säkerhetsutredningar breddas och en utredning får också bygga på vissa uppgifter i register som förs av en myndighet i en annan stat (25 §). I lagen finns också en uttömmande uppräkning över de register som får användas vid utredningsförfarandet.

I den nya lagen finns det bestämmelser också om säkerhetsutredningar av företag. I 33 § bestäms om rätten att ansöka om säkerhetsutredning av företag och i 36 § om förutsättningar för säkerhetsutredning av företag. I 37 § förtecknas informationskällorna vid säkerhetsutredning av företag och 38 § handlar om handläggning av säkerhetsutredningar av företag. Vid en säkerhetsutredning av företag ska det med hjälp av uppgifterna i ansökan och de informationskällor som avses i 37 § samt genom inspektion av företaget och dess verksamhetsutrymmen samt dess informationssystem och datakommunikation klarläggas hur företaget kan sörja för säkerhetsarrangemangen (38 § 1 mom.). I praktiken deltar två behöriga myndigheter i uppdraget, eftersom det ankommer på Kommunikationsverket att bedöma informationssäkerheten i informationssystem och datakommunikation. Med hjälp av de metoder som står till förfogande för de behöriga myndigheterna klarläggs det hur företaget kan sörja för olika omständigheter som hänför sig till informationssäkerheten. Den behöriga myndigheten kan när den gör en säkerhetsutredning av företag och upprättar ett intyg över utredningen förutsätta att näringsidkaren förbinder sig att sörja för att informationssäkerhetsnivån bevaras (40 §).

3 Målsättning och de viktigaste förslagen

Propositionen syftar till att inhämta riksdagens godkännande för överenskommelsen. Överenskommelsen syftar till att säkerställa att säkerhetsklassificerad information som Finland lämnar ut till Kroatien skyddas och hanteras korrekt. Överenskommelsen syftar också till att främja Finlands möjligheter att ta emot säkerhetsklassificerad information från Kroatien och så förbättra samarbetet mellan länderna inom informationssäkerhetsområdet. Ytterligare syftar överenskommelsen till att trygga finländska företags möjligheter att delta i internationella projekt eller projekt mellan Finland och Kroatien som kan kräva utbyte av säkerhetsklassificerad information och på det sättet till att förbättra de finländska företagens konkurrenskraft. Propositionen innehåller också ett förslag till så kallad blankettlag, genom vilken de bestämmelser i överenskommelsen som hör till området för lagstiftningen sätts i kraft.

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 (särskilt känsligt informationsmaterial) som skickas från Kroatien till Finland. Skyddet av särskilt känsligt informationsmaterial i enlighet med lagen om internationella förpliktelser som gäller informationssäkerhet utgår från bestämmelserna i överenskommelsen.

Särskilt känsligt informationsmaterial enligt överenskommelsen mellan Finland och Kroatien är handlingar som Kroatien anser att ska vara sekretessbelagda och följaktligen har bestämt att ska ha hög säkerhetsklassificering och försett med sådan anteckning. I artikel 5 i överenskommelsen föreskrivs om sekretessen avseende säkerhetsklassificerad information. Enligt artikel 5.9 a ska den mottagande parten förmedla säkerhetsklassificerad information till tredje parter endast med skriftligt förhandssamtycke av den utlämnande parten. Detta utgör ett undantag till bestämmelserna i offentlighetslagen om sekretessbeläggning i allmänt intresse, eftersom sekretessen där i de flesta fall är beroende av konsekvenserna för det skyddade intresset, om uppgifterna lämnas ut. Även utan överenskommelse om informationssäkerhet skulle säkerhetsklassificerade handlingar som Kroatien lämnar ut till Finland i regel sekretessbeläggas med stöd av 24 § 1 mom. 2 punkten i offentlighetslagen, vilket innebär att överenskommelsen om informationssäkerhet inte begränsar allmänhetens tillgång till information dess mera än offentlighetslagen.

Den största skillnaden består i att en myndighet som ska avgöra en begäran om att få ta del av information i en handling som avses

i en internationell förpliktelse om informationssäkerhet inte särskilt behöver motivera den skada som orsakas av att informationen ges ut. I övrigt ska en begäran om information behandlas i enlighet med offentlighetslagen. Uppkommer det oklarheter om huruvida klassificeringen är korrekt eller om vilka uppgifter i handlingen det är som föranleder klassificeringen, ska myndigheten kontakta den part som har upprättat handlingen.

Överenskommelsen om informationssäkerhet mellan Finland och Kroatien inverkar inte på sekretessen eller klassificeringen av Finlands nationella handlingar, vilka bestäms utifrån offentlighetslagen.

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

4.2 Konsekvenser för näringslivet

Överenskommelsen öppnar möjligheter för finländska företag att få beställningar eller att delta i projekt som förutsätter tillgång till information som är säkerhetsklassificerad i Kroatien. Analogt öppnar överenskommelsen möjligheter för kroatiska företag att få beställningar eller att delta i projekt som förutsätter tillgång till information som är säkerhetsklassificerad i Finland. Det är svårt att på förhand uppskatta antalet och det ekonomiska värdet på kommande projekt. Projekt som kräver tillgång till säkerhetsklassificerad information förekommer särskilt inom försvarsindustrin, säkerhetssektorn, kärnkraft, informationsteknologi och annan högteknologi samt inom sektorn för vetenskap och forskning. Utan överenskommelse om informationssäkerhet kan finländska företag ställas utanför kroatiska projekt. Överenskommelsen syftar just till att bygga upp mekanismer och förfaranden på förhand för att det ska vara möjligt att delta i projekt och till att på detta sätt förbättra finländska företags konkurrenskraft.

4.3 Ekonomiska konsekvenser

Propositionen har inga konsekvenser för statsbudgeten eller andra 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. Överenskommelsen ökar i någon mån den nationella säkerhetsmyndighetens och de utsedda säkerhetsmyndigheternas uppgifter som enligt 4 § i lagen om internationella förpliktelser som gäller informationssäkerhet hör till dessa myndigheter.

5 Beredningen av propositionen

Propositionen har beretts vid utrikesministeriet. I beredningen av och i förhandlingarna om överenskommelsen deltog representanter för utrikesministeriet, justitieministeriet, försvarsministeriet och Skyddspolisen. Yttranden om propositionen begärdes av arbets- och näringsministeriet, finansministeriet, försvarsministeriet, inrikesministeriet, justitieministeriet, kommunikationsministeriet, Kommunikationsverket och Skyddspolisen. Yttranden lämnades av försvarsministeriet, inrikesministeriet, kommunikationsministeriet samt av Skyddspolisen. Inrikesministeriet önskade i sitt yttrande att propositionens motiveringar preciseras med avseende på polisens undersöknings- och underrättelseinformation. Yttrandet har beaktats i detaljmotiveringen för artikel 1 om överenskommelsens mål. Yttrandena förordar att överenskommelsen godkänns och sätts ikraft.

DETALJMOTIVERING

1 Överenskommelsens innehåll och förhållande till lagstiftningen i Finland

Artikel 1. *Mål.* Artikeln fastställer att målet med överenskommelsen är att skydda sådan säkerhetsklassificerad information som framställs eller utbyts mellan parterna. I inledningen till överenskommelsen anges att parternas samarbetsområden omfattar utrikes-, försvars-, säkerhets- och polisfrågor samt vetenskaps-, näringslivs- och teknologifrågor. Överenskommelsen tillämpas inte på utbyte mellan parterna av information som inte är säkerhetsklassificerad. I Finland görs det till exempel i regel inte anteckning om säkerhetsklassificering i polisens undersöknings- och underrättelseinformation.

Artikel 2. *Definitioner*. I artikeln definieras de begrepp som är centrala i tillämpningen av överenskommelsen på följande sätt:

I punkt 1 definieras säkerhetsklassificerad information. Överenskommelsen gäller all information, oavsett form, som ska skyddas mot dataskyddskränkningar och som har klassificerats i enlighet med den utlämnande partens nationella lagar och bestämmelser. Punkten är i samklang med definitionen i 2 § 1 mom. i lagen om internationella förpliktelser som gäller informationssäkerhet.

Enligt punkt 2 avses med informationsbehov behov av tillgång till säkerhetsklassificerad information i en bestämd officiell position eller för att uträtta en bestämd uppgift.

Enligt punkt 3 avses med kränkning av dataskyddet alla former av röjande, ändring, missbruk, skadande eller förstörande av säkerhetsklassificerad information utan tillåtelse eller andra sådana handlingar eller försummelser som kan leda till att informationens sekretess, integritet eller användbarhet går förlorad.

Enligt punkt 4 avses med säkerhetsklass en kategori som i enlighet med nationella lagar och bestämmelser uttrycker hur begränsad tillången till den säkerhetsklassificerade informationen är samt parternas minimiskyddsnivå för denna information.

I enlighet med punkt 5 avses med utlämnande part den part som lämnar ut säkerhetsklassificerad information eller under vilken säkerhetsklassificerad information framställs.

I enlighet med punkt 6 avses med mottagande part den part till vilken den utlämnande partens säkerhetsklassificerade information lämnas ut. Definitionen omfattar också offentlig- eller privaträttsliga juridiska och fysiska personer inom partens jurisdiktion.

Enligt punkt 7 avses med nationell säkerhetsmyndighet den nationella myndighet som ansvarar för genomförandet och övervakningen av överenskommelsen.

Enligt punkt 8 avses med behörig säkerhetsmyndighet en nationell säkerhetsmyndighet, en utsedd säkerhetsmyndighet eller en nationell informationssäkerhetsmyndighet eller någon annan nationell myndighet som i enlighet med nationella lagar och bestämmelser genomför överenskommelsen.

Enligt punkt 9 avses med kontraktspart fysisk eller juridisk person som har rättslig behörighet att ingå kontrakt.

Enligt punkt 10 avses med säkerhetsklassificerat kontrakt en överenskommelse mellan två eller flera kontraktsparter som inbegriper eller vars genomförande kräver tillgång till säkerhetsklassificerad information. Punkten är i samklang med definitionen i 2 § 1 mom. i lagen om internationella förpliktelser som gäller informationssäkerhet.

Enligt punkt 11 avses med säkerhetsutredning av person en bedömning i enlighet med nationella lagar och bestämmelser av den behöriga säkerhetsmyndigheten, enligt vilken

en fysisk person kan beviljas tillgång till säkerhetsklassificerad information.

Enligt punkt 12 avses med säkerhetsutredning som gäller sammanslutning en bedömning av den behöriga säkerhetsmyndigheten som i enlighet med den berörda partens nationella lagar och bestämmelser bekräftar att en fysisk eller juridisk person uppfyller förutsättningarna för tillgång till och handläggning av säkerhetsklassificerad information.

Enligt punkt 13 avses med tredje part en stat, organisation, juridisk eller fysisk person, som inte är part i överenskommelsen.

Artikel 3. *Säkerhetsklasser*. Enligt punkt 1 ska säkerhetsklassificerad information som lämnas ut i enlighet med överenskommelsen förses med relevant anteckning om säkerhetsklass i enlighet med parternas lagar och bestämmelser.

I punkt 2 definieras hur Finlands och Kroatiens säkerhetsklasser motsvarar varandra. Den högsta säkerhetsklassen, som kräver de strängaste informationssäkerhetsåtgärderna, är ”ERITTÄIN SALAINEN/YTTERST HEMLIG” (VRLO TAJNO). Till denna kategori räknas i Finland information som, om den obehörigen röjs, kan orsaka särskilt påtaglig skada för försvaret, säkerheten, de internationella relationerna eller andra allmänna intressen. Den nästhögsta säkerhetsklassen är ”SALAINEN/HEMLIG” (TAJNO). Hit hör i Finland information som, om den obehörigen röjs, kan orsaka väsentlig skada för försvaret, säkerheten, de internationella relationerna eller andra allmänna intressen. Den tredje högsta säkerhetsklassen är "LUOTTAMUKSELLINEN/KONFIDENTIELL" (POVJERLJIVO), 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 handlingar, "KÄYTTÖ RAJOITETTU/BEGRÄNSAD TILLGÅNG" (OGRANIČENO) hör information som, om den obehörigen röjs, kan skada allmänna intressen eller försämra myndigheternas möjligheter att agera.

Finlands internationella relationer skyddas i 24 § 1 mom. 1 och 2 punkten i offentlighetslagen, försvaret i punkt 10 och säkerheten i punkt 5, 8 och 9 i samma moment. Andra allmänna intressen som avses i offentlighetslagen kan t.ex. vara skyddet av säkerhetsarrangemangen för statsledningen och statsbesök och för datasystem (24 § 1 mom. 7 punkten) samt samhällsekonomin (24 § 1 mom. 11 och 12 punkten). Allmänt tillämpliga bestämmelser om sekretess- och klassificeringsanteckningar i myndighetshandlingar ingår i 25 § i offentlighetslagen. Enligt 25 § 3 mom. kan en handling förses med en anteckning som anger vilka krav på datasäkerhet som ska följas vid hanteringen av handlingen. Handlingar som avses i lagen om internationella förpliktelser som gäller informationssäkerhet ska förses med anteckning om säkerhetsklass i enlighet med den lagen. Anteckning om säkerhetsklassificering ska göras också om det föreskrivs genom förordning av statsrådet.

Enligt 8 § i lagen om internationella förpliktelser som gäller informationssäkerhet ska särskilt känsligt informationsmaterial, oberoende av vad som föreskrivs i lagen om offentlighet i myndigheternas verksamhet, förses med en sådan anteckning om säkerhetsklass som anges i en internationell förpliktelse som gäller informationssäkerhet, för att ange vilka säkerhetskrav som ska följas vid hanteringen av materialet. Särskilda bestämmelser om anteckningen om säkerhetsklassificering finns i 11 § i informationssäkerhetsförordningen och föreskrifter om klassificeringens motsvarighet vid tillgodoseendet av internationella förpliktelser som gäller informationssäkerheten i 12 § i förordningen. I 11 § 1 mom. i förordningen föreskrivs det när en anteckning om säkerhetsklassificering kan göras i en sekretessbelagd handling. Enligt 11 § 3 mom. får anteckning om säkerhetsklass inte användas i andra fall än de som avses i 1 mom., om inte anteckningen är nödvändig för tillgodoseendet av en internationell förpliktelse som gäller informationssäkerhet eller handlingen i övrigt hänför sig till internationellt samarbete. I 11 § 4 mom. i förordningen finns en specialbestämmelse om anteckning om säkerhetsklassificering på svenska.

Enligt punkt 3 ska den mottagande parten säkerställa att säkerhetsklasser inte ändras el-

ler upphävs utan skriftligt tillstånd av den utlämnande parten.

Artikel 4. *Behöriga säkerhetsmyndigheter.* I punkt 1 anges vardera partens utsedda nationella säkerhetsmyndigheter (National Security Authority, NSA) som ansvarar för det allmänna genomförandet av överenskommelsen. Nationell säkerhetsmyndighet i Finland är enligt 4 § i lagen om internationella förpliktelser som gäller informationssäkerhet utrikesministeriet, där uppgiften sköts av Nationella säkerhetsmyndigheten (NSA). I Kroatien har Office of the National Security Council utsetts till nationell säkerhetsmyndighet.

I punkt 2 förpliktas parterna att underrätta varandra om eventuella ändringar i de nationella säkerhetsmyndigheterna. De nationella säkerhetsmyndigheterna ska underrätta varandra om eventuella andra behöriga säkerhetsmyndigheter (Competent Security Authorities, CSA) och om senare ändringar som avser dem. Utsedda säkerhetsmyndigheter (Designated Security Authority, DSA) i Finland är enligt 4 § i lagen om internationella förpliktelser som gäller informationssäkerhet försvarsministeriet, huvudstaben, Skyddspolisen och Kommunikationsverket.

I punkt 3 förpliktas parterna att underrätta varandra om gällande nationella lagar och bestämmelser som reglerar skyddet av säkerhetsklassificerad information och att på begäran utbyta information angående säkerhetsstandarder, -förfaranden och -praxis för skyddet av säkerhetsklassificerad information.

Artikel 5. *Skyddsåtgärder och tillgång till säkerhetsklassificerad information.* Artikeln innehåller de viktigaste förpliktelserna om ömsesidigt skydd.

I punkt 1 förpliktas parterna att vidta alla lämpliga åtgärder i enlighet med sina nationella lagar och bestämmelser för att skydda säkerhetsklassificerad information som framställts eller utbytts i enlighet med överenskommelsen och ge den skydd på samma nivå som egen information i motsvarande säkerhetsklass.

Enligt punkt 2 ska den utlämnande parten skriftligen underrätta den mottagande parten om ändringar i säkerhetsklassen för utlämnad säkerhetsklassificerad information för att den mottagande parten ska tillämpa lämpliga säkerhetsåtgärder.

Punkt 3 gäller personalsäkerhet. Enligt den ska tillgång till säkerhetsklassificerad information endast beviljas fysiska personer som har ett informationsbehov, som har utfärdats en lämplig säkerhetsutredning av person i enlighet med nationella lagar och bestämmelser och som har fått instruktioner om sitt ansvar i skyddet av säkerhetsklassificerad information. Bestämmelsen är i samklang med 6 § 3 mom. i lagen om internationella förpliktelser som gäller informationssäkerhet, enligt vilken endast personer som behöver informationen för skötsel av sina uppgifter ska ha tillgång till materialet. Den kontroll av en persons tillförlitlighet som internationella informationssäkerhetsförpliktelser kräver utförs i Finland i enlighet med lagen om säkerhetsutredningar och med 11 § i lagen om internationella förpliktelser som gäller informationssäkerhet. När lagändringarna har trätt i kraft den 1 januari 2015 görs en säkerhetsutredning av person på det sätt som föreskrivs i den nya säkerhetsutredningslagen och intyg över säkerhetsutredning av person utfärdas i enlighet med lagen om internationella förpliktelser som gäller informationssäkerhet (ändrade 11 §).

Enligt punkt 4 krävs de inte någon säkerhetsutredning av person för tillgång till säkerhetsklassificerad information i säkerhetsklass KÄYTTÖ RAJOITETTU/BEGRÄNSAD TILLGÅNG/OGRANIČENO.

Enligt punkt 5 erkänner bägge parter säkerhetsutredningar av personer eller sammanslutningar utfärdade av den andra parten.

Enligt punkt 6 bistår de behöriga säkerhetsmyndigheterna varandra på begäran och i enlighet med sina nationella lagar och bestämmelser med utredningsförfaranden som behövs för tillämpningen av överenskommelsen. Detta bistånd kan förutsätta informationsutbyte som har betydelse med avseende på 17 § i lagen om internationella förpliktelser som gäller informationssäkerhet. Enligt den paragrafen har finska myndigheter rätt att till en annan fördragsslutande part lämna ut handlingar och information som behövs

för uppfyllande av en internationell förpliktelse som gäller informationssäkerhet, oavsett vad som i finsk lagstiftning föreskrivs om sekretessbeläggning av handlingar och uppgifter. Detta gäller emellertid inte uppgifter som är sekretessbelagda för tryggande av integritetsskyddet. Enligt den nya säkerhetsutredningslagen får en säkerhetsutredning av person inkludera vissa uppgifter som har registrerats i informationssystemet hos en annan stats myndigheter (25 och 26 §).

I punkt 7 förpliktas de nationella säkerhetsmyndigheterna att utan dröjsmål underrätta varandra om ändringar i säkerhetsutredningar som avser personer eller sammanslutningar.

Enligt punkt 8 ska den mottagande partens nationella säkerhetsmyndighet på begäran av den utlämnande partens nationella säkerhetsmyndighet ge en skriftlig bekräftelse på att en fysisk person har rätt att få tillgång till säkerhetsklassificerad information eller på att en juridisk person har utfärdats en säkerhetsutredning som gäller sammanslutning.

Punkt 9 a förbjuder utlämnande av säkerhetsklassificerad information till tredje parter utan skriftligt förhandssamtycke av den utlämnande parten. Punkten förpliktar parterna att följa principen om utlämnarens samtycke.

Enligt punkt 9 b ska den mottagande parten märka mottagen säkerhetsklassificerad information i enlighet med säkerhetsklassmotsvarigheten i artikel 3. En bestämmelse som motsvarar förpliktelsen finns i 8 § 1 mom. i lagen om internationella förpliktelser om informationssäkerhet.

Enligt punkt 9 c får säkerhetsklassificerad information endast användas för de ändamål den har utlämnats för. En bestämmelse som motsvarar förpliktelsen finns i 6 § 2 mom. i lagen om internationella förpliktelser om informationssäkerhet.

Enligt punkt 10 ska, om det i någon annan överenskommelse mellan parterna förekommer strängare bestämmelser om utbyte eller skydd av säkerhetsklassificerad information, dessa strängare bestämmelser tillämpas.

Artikel 6. *Förmedling av säkerhetsklassificerad information.* Artikeln innehåller bestämmelserna om förfarandet vid överföring av säkerhetsklassificerad information mellan parterna.

Säkerhetsklassificerad information förmedlas enligt punkt 1 via kanaler som de behöriga säkerhetsmyndigheterna har godkänt. Den mottagande parten ska bekräfta mottagandet av säkerhetsklassificerad information i säkerhetsklass SALAINEN/HEMLIG/TAJNO och högre.

Enligt punkt 2 förmedlas säkerhetsklassificerad information elektroniskt endast på ett sådant säkert sätt som de behöriga säkerhetsmyndigheterna sinsemellan har kommit överens om.

Artikelns bestämmelser är i samklang med 18 § i informationssäkerhetsförordningen om förmedling av en handling och med 19 § om överföring av en handling i datanätet.

Artikel 7. *Kopiering och översättning av säkerhetsklassificerad information.* Artikeln innehåller bestämmelser om hur material i olika säkerhetsklasser får kopieras och översättas.

Enligt punkt 1 får information i säkerhetsklass ERITTÄIN SALAINEN/YTTERSTHEMLIG/VRLO TAJNO översättas eller kopieras endast i undantagsfall, med den utlämnande partens skriftliga förhandssamtycke.

I punkt 2 förpliktas parterna att förse alla kopior av säkerhetsklassificerad information med den ursprungliga klassificeringsanteckningen. Sådan kopierad information ska skyddas på samma sätt som den ursprungliga informationen. Antalet kopior ska begränsas till vad det officiella syftet kräver.

I punkt 3 förpliktas parterna att förse översättningar med samma klassificeringsanteckning som originalet och dessutom med en anmärkning på översättningsspråket om att översättningen innehåller säkerhetsklassificerad information från den utlämnande parten.

Bestämmelser om skyldigheten att se till att särskilt känsligt informationsmaterial skyddas på ett sätt som motsvarar säkerhetsklassen när sådant material produceras, kopieras, översänds, distribueras, lagras, utplånas eller i något annat avseende hanteras finns i 9 § 1 mom. i lagen om internationella förpliktelser som gäller informationssäkerhet. De närmare bestämmelserna om hanteringen regleras i

Finland på förordningsnivå. I 17 § i informationssäkerhetsförordningen som har utfärdats med stöd av offentlighetslagen bestäms om kopiering av handlingar.

Artikel 8. *Utplåning av säkerhetsklassificerad information.* Artikeln innehåller bestämmelser om hur material i olika säkerhetsklasser får utplånas.

Enligt punkt 1 ska informationen utplånas så att det förhindras att informationen helt eller delvis framställs på nytt.

Enligt punkt 2 utplånas information i säkerhetsklass ERITTÄIN SALAINEN/YTTERST HEMLIG/VRLO TAJNO inte, utan återlämnas till den utlämnande parten.

Enligt punkt 3 kan den utlämnande parten uttryckligen förbjuda utplåning av säkerhetsklassificerad information. I det fallet återlämnas informationen till den utlämnande parten.

Enligt punkt 4 ska i krissituationer som gör det omöjligt att skydda eller återlämna säkerhetsklassificerad information som framställts eller utbytts i enlighet med överenskommelsen informationen omedelbart utplånas. Den mottagande parten ska så fort som möjligt underrätta den utlämnande partens nationella säkerhetsmyndighet om att informationen har utplånats.

Bestämmelser om skyldigheten att se till att särskilt känsligt informationsmaterial skyddas på ett sätt som motsvarar säkerhetsklassen när sådant material produceras, kopieras, översänds, distribueras, lagras, utplånas eller i något annat avseende hanteras finns i 9 § 1 mom. i lagen om internationella förpliktelser som gäller informationssäkerhet. De närmare bestämmelserna om hanteringen regleras i Finland på förordningsnivå. I 21 § i informationssäkerhetsförordningen som har utfärdats med stöd av offentlighetslagen bestäms om arkivering och utplåning av handlingar.

Artikel 9. *Säkerhetsklassificerade kontrakt.* Artikeln innehåller bestämmelser om ingående inom någondera partens territorium av säkerhetsklassificerade kontrakt som avses i artikel 2.10.

Enligt punkt 1 ingås och verkställs säkerhetsklassificerade kontrakt i enlighet med bägge parters nationella lagar och bestämmelser.

Enligt punkt 2 ska den mottagande partens nationella säkerhetsmyndighet på begäran bekräfta att en föreslagen kontraktspart har utfärdats en lämplig säkerhetsutredning av person eller sammanslutning. Om kontraktsparten inte har någon lämplig säkerhetsutredning, kan den utlämnande partens nationella säkerhetsmyndighet begära att den mottagande partens behöriga säkerhetsmyndighet utfärdar en sådan.

Enligt punkt 3 krävs ingen säkerhetsutredning som gäller sammanslutning för säkerhetsklassificerade kontrakt i säkerhetsklassen KÄYTTÖ RAJOITETTU/BEGRÄNSAD TILLGÅNG/ OGRANIČENO.

Punkt 4 förpliktar parterna att i säkerhetsklassificerade kontrakt inkludera lämpliga säkerhetsbestämmelser, där den utlämnande parten specificerar den säkerhetsklassificerade information som utlämnas till den mottagande parten, informationens säkerhetsklass samt kontraktspartens skyldigheter med avseende på skyddet av den säkerhetsklassificerade informationen.

I punkt 5 finns en förteckning över kontraktsparters minimiförpliktelser i skyddet av säkerhetsklassificerad information.

Nationella bestämmelser om säkerhetsklassificerade kontrakt finns i 1 § 2 mom. (tilllämpning på näringsidkare), 2 § 2 punkten (särskilt känsligt informationsmaterial), 7 § (tystnadsplikt och förbud mot utnyttjande) samt i 12 § (säkerhetsutredningar som gäller sammanslutningar), 13 § (förbindelse om att vidta säkerhetsåtgärder) och 14 § (säkerhetsintyg) i lagen om internationella förpliktelser som gäller informationssäkerhet. När ändringarna i lagen om internationella förpliktelser som gäller informationssäkerhet har trätt i kraft föreskrivs det i 12 § om intyg över säkerhetsutredning av företag, dess giltighet och återkallelse och i 14 § om anteckning av uppgifter om intyg i registret över säkerhetsutredningar. Lagens 13 § om förbindelse upphävs, men motsvarande bestämmelse ingår i den nya säkerhetsutredningslagen (40 §). Den nationella regleringen motsvarar förpliktelserna i överenskommelsen. Finska myndigheters rätt att lämna ut information

som är nödvändig för att uppfylla förpliktelsen finns föreskriven i 17 § i lagen om internationella förpliktelser som gäller informationssäkerhet.

Enligt punkt 6 ska underleverantörer följa de säkerhetsbestämmelser som tillämpas på kontraktsparter.

Artikel 10. *Besök.* Artikeln tillämpas på besök som omfattar tillgång till säkerhetsklassificerad information.

Enligt punkt 1 behövs det ett förhandstillstånd av värdpartens behöriga säkerhetsmyndighet för sådana besök. Tillståndet beviljas utifrån en besöksbegäran av den besökande partens nationella säkerhetsmyndighet.

I punkt 2 finns en förteckning över de uppgifter en besöksbegäran ska innehålla.

Punkt 3 innehåller bestämmelserna om de förfaranden som ska följas vid besök. Enligt tidsfristen som anges i punkten ska besöksbegäran framföras minst tre veckor i förväg. I brådskande fall kan de behöriga säkerhetsmyndigheterna komma överens om en kortare tidsfrist.

Enligt punkt 4 ska vardera parten garantera skyddet av besökarnas personuppgifter i enlighet med sina nationella lagar och bestämmelser.

Artikel 11. *Kränkning av dataskyddet.*

I punkt 1 förpliktas de nationella säkerhetsmyndigheterna att utan dröjsmål underrätta varandra om kränkningar av dataskyddet och inleda ett lämpligt förfarande i enlighet med sina nationella lagar och bestämmelser för att fastställa omständigheterna kring kränkningen. Resultatet av förfarandet ska lämnas till den utlämnande partens nationella säkerhetsmyndighet.

Enligt punkt 2 ska, om kränkningen av dataskyddet sker i en tredje stat, den part som har sänt ut informationen vidta åtgärderna enligt punkt 1.

Bestämmelser som rör förpliktelserna i artikeln ingår i 19 § i lagen om internationella förpliktelser som gäller informationssäkerhet.

Artikel 12. *Kostnader.* Enligt artikeln står vardera parten för sina egna kostnader som genomförandet och övervakningen av överenskommelsen medför.

Artikel 13. *Tvistlösning.* Enligt artikeln ska alla tvister om tolkningen eller tillämpningen av överenskommelsen avgöras enbart genom samråd mellan parterna och inte hänskjutas till någon internationell domstol eller tredje part för avgörande.

Artikel 14. *Slutbestämmelser.* I artikeln ingår bestämmelser om ikraftträdande, ändringar och uppsägning av överenskommelsen samt om skyldigheter som följer av en uppsägning. Överenskommelsen gäller tills vidare. Den kan ändras på gemensam skriftlig överenskommelse mellan parterna. Vardera parten kan säga upp överenskommelsen genom skriftlig anmälan till den andra parten via diplomatiska kanaler, iakttagande en uppsägningstid på sex månader.

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 överenskommelsen om informationssäkerhet mellan Finland och Kroatien, innehåller propositionen endast ett förslag till en blankettlag.

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

2 §. Om sättande i kraft av de bestämmelser i överenskommelsen som inte hör till området för lagstiftningen och om ikraftträdandet av lagen bestäms genom förordning av statsrådet. Lagen avses träda i kraft samtidigt som överenskommelsen träder i kraft för Finlands del.

3 Ikraftträdande

Enligt artikel 14.1 i överenskommelsen mellan Finland och Kroatien träder överenskommelsen i kraft den första dagen i den

andra månaden efter att den senare skriftliga underrättelsen har mottagits där parterna via diplomatiska kanaler meddelar varandra att de nationella rättsliga kraven som ikraftträdandet av överenskommelsen förutsätter har uppfyllts.

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 statsrådet.

4 Behovet av riksdagens samtycke och behandlingsordning

4.1 Behovet av riksdagens samtycke

Enligt 94 § 1 mom. i grundlagen krävs riksdagens godkännande för fördrag och andra internationella förpliktelser som innehåller 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 anförs ovan krävs riksdagens samtycke för flera bestämmelser i överenskommelsen som ingår i propositionen. I artikel 2 definieras bland annat vad som avses med säkerhetsklassificerad information, säkerhetsklassificerade kontrakt, säkerhetsutredningar och kränkning av dataskyddet. Eftersom dessa definitioner direkt eller indirekt påverkar tolkningen och tillämpningen av materiella bestämmelser i överenskommelsen som hör till området för lagstiftningen kräver de riksdagens godkännande (GrUU 6/2001 rd).

Artikel 3 innehåller bestämmelser om anteckningar om säkerhetsklassificering och om säkerhetsklassernas motsvarighet. Allmänt tillämpliga bestämmelser om anteckningar om sekretess och klassificering ingår i 25 § i offentlighetslagen. Enligt den ska det göras en sekretessanteckning 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 en anteckning göras efter prövning. I 8 § i lagen om internationella förpliktelser som gäller informationssäkerhet finns det dessutom bestämmelser om anteckning av säkerhetsklass i särskilt känsligt informationsmaterial. Enligt den ska särskilt känsligt informationsmaterial oberoende av vad som föreskrivs i offentlighetslagen förses med en sådan anteckning om säkerhetsklass som anges i en internationell förpliktelse som gäller informationssäkerhet, för att ange vilka säkerhetskrav som ska följas vid hantering av materialet. Bestämmelsen hör till området för lagstiftningen.

I artikel 4 ställs det fast att utrikesministeriet är Finlands nationella säkerhetsmyndighet. Bestämmelsen motsvarar 4 § 1 mom. i lagen om internationella förpliktelser som gäller informationssäkerhet. Bestämmelsen är konstaterande och ska därför inte anses förutsätta riksdagens samtycke.

I artikel 5 i överenskommelsen föreskrivs om åtgärder som krävs för att skydda säkerhetsklassificerad information inom tillämpningsområdet för överenskommelsen och som begränsar utlämnande, förmedling och användning av samt tillgången till informationen. Artikel 5.9 a utgör kärnan i överenskommelsen, utifrån vilken Finland kan skydda säkerhetsklassificerad information som utbyts med stöd av överenskommelsen utan den skaderekvisitbedömning som föreskrivs i offentlighetslagen. I Finland är myndighetshandlingar enligt huvudregeln offentliga. Var och en har enligt 12 § 2 mom. i grundlagen rätt att ta del av myndigheters offentliga handlingar. Denna rätt kan endast av tvingande skäl begränsas genom lag. Avvikande

från bestämmelserna i offentlighetslagen ska särskilt känsligt informationsmaterial enligt 6 § 1 mom. i lagen om internationella förpliktelser som gäller informationssäkerhet sekretessbeläggas, om inte annat följer av en internationell förpliktelse som gäller informationssäkerhet. I artikel 5.3 anges också en begränsning med avseende på personer som ska få tillgång till säkerhetsklassificerad information. I punkten föreskrivs också om parternas skyldighet att låta utföra en lämplig säkerhetsutredning över personer som har eller kan ha tillgång till säkerhetsklassificerad information som avses i överenskommelsen. I upplägget för säkerhetsutredningar ska det som sägs i 10 § 1 mom. i grundlagen om tryggat privatliv och om plikten att lagstifta om skydd för personuppgifter beaktas. I Finland finns det i lagen om säkerhetsutredningar föreskrifter om vilka som ska vara föremål för säkerhetsutredningar samt om utredningsförfarandet (från den 1 januari 2015 i säkerhetsutredningslagen). Bestämmelsen hör följaktligen till området för lagstiftningen och kräver riksdagens samtycke för att träda i kraft. Enligt artikel 5.9 c får säkerhetsklassificerad information endast användas för de ändamål den har utlämnats för. En bestämmelse som motsvarar förpliktelsen finns i 6 § 2 mom. i lagen om internationella förpliktelser om informationssäkerhet. Bestämmelsen i denna punkt hör följaktligen till området för lagstiftningen.

I artikel 9 i överenskommelsen finns det bestämmelser om säkerhetsklassificerade kontrakt och om säkerhetsutredningar som gäller företag som är parter i sådana kontrakt. Föreskrifter om säkerhetsutredningar som gäller sammanslutningar finns i 12 och 13 § i lagen om internationella förpliktelser om informationssäkerhet. Motsvarande bestämmelser ingår i säkerhetsutredningslagen som träder i kraft den 1 januari 2015. Samtidigt ändras 11 och 12 § i lagen om internationella förpliktelser om informationssäkerhet så att 11 § gäller intyg över säkerhetsutredning av person, dess giltighet och återkallelse och 12 § intyg över säkerhetsutredning av företag, dess giltighet och återkallelse. Bestämmelserna om säkerhetsklassificerade kontrakt och intyg över säkerhetsutredning av företag hör följaktligen till området för lagstiftningen.

I punkt 11 i överenskommelsen förutsätts att de nationella säkerhetsmyndigheterna utan dröjsmål underrättar varandra om kränkningar av dataskyddet och inleder ett lämpligt förfarande i enlighet med sina nationella lagar och bestämmelser för att fastställa omständigheterna kring kränkningen. Resultatet av förfarandet ska lämnas till den utlämnande partens nationella säkerhetsmyndighet. I 19 § i lagen om internationella förpliktelser som gäller informationssäkerhet föreskrivs om de nationella säkerhetsmyndigheternas skyldigheter i sådana situationer som avses i bestämmelserna i överenskommelsen. Artikelns bestämmelser hör följaktligen till området för lagstiftningen.

4.2 Behandlingsordning

Allmänt tillämpliga bestämmelser om sekretess avseende säkerhetsklassificerade uppgifter finns i lagen om internationella förpliktelser som gäller informationssäkerhet. Enligt 6 § 1 mom. i den lagen ska särskilt känsligt informationsmaterial sekretessbeläggas, om inte annat följer av en internationell förpliktelse som gäller informationssäkerhet. Enligt 6 § 2 mom. får särskilt känsligt informationsmaterial användas och lämnas ut endast för angivet ändamål, om inte den som bestämt materialets säkerhetsklass har samtyckt till något annat. Vidare ska enligt 6 § 3 mom. en myndighet som hanterar särskilt känsligt informationsmaterial se till att endast personer som behöver informationen för skötseln av sina uppgifter har tillgång till materialet. Dessa personer ska i de fall som den internationella förpliktelsen som gäller informationssäkerhet förutsätter namnges på förhand. Detsamma gäller näringsidkare som avses i 1 § 2 mom. Med särskilt känsligt informationsmaterial avses i lagen sådana sekretessbelagda handlingar och material samt sådan information som kan fås ur dem samt sådana handlingar och material som producerats utifrån dessa handlingar och material samt denna information och som har säkerhetsklassificerats enligt en internationell förpliktelse som gäller informationssäkerhet. Be-

stämmelserna i artikel 5 i den föreliggande överenskommelsen breddar inte skyldigheten att iaktta sekretess från vad som har reglerats i 6 § i nämnda lag. Bestämmelserna inverkar följaktligen inte på behandlingsordningen av överenskommelsen.

Överenskommelsen mellan Finland och Kroatien om ömsesidigt skydd av säkerhetsklassificerad information kan inte anses innehålla bestämmelser som berör grundlagen på det sätt som avses i 94 § 2 mom. och 95 § 2 mom. i grundlagen. Enligt regeringens uppfattning kan överenskommelsen följaktligen godkännas med enkel majoritet och förslaget om sättande i kraft av de bestämmelser i överenskommelsen som hör till området för lagstiftningen godkännas i vanlig lagstiftningsordning.

Med stöd av vad som anförts ovan och i enlighet med 94 § i grundlagen föreslås att

riksdagen godkänner den i Zagreb den 11 februari 2014 mellan Republiken Finlands regering och Republiken Kroatiens regering upprättade överenskommelsen om ömsesidigt skydd av säkerhetsklassificerad information.

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

Lagförslag

Lag

Lag om sättande i kraft av de bestämmelser i överenskommelsen med Kroatien om ömsesidigt skydd av säkerhetsklassificerad information som hör till området för lagstiftningen

I enlighet med riksdagens beslut föreskrivs:

1 §

De bestämmelser som hör till området för lagstiftningen i den i Zagreb den 11 februari 2014 mellan Republiken Finlands regering och Republiken Kroatiens regering upprättade överenskommelsen om ömsesidigt skydd av säkerhetsklassificerad information gäller som lag sådana Finland har förbundit sig till dem.

2 §

Om sättande i kraft av de övriga bestämmelserna i överenskommelsen och om ikraftträdandet av denna lag bestäms genom förordning av statsrådet.

Helsingfors den 4 december 2014

Statsminister

ALEXANDER STUBB

Utrikesråd *Maarit Jalava*

Översättning *Fördragstext*

ÖVERENSKOMMELSE MELLAN REPUBLIKEN FINLANDS REGERING OCH REPUBLIKEN KROATIENS REGERING OM ÖMSESIDIGT SKYDD AV SÄKERHETSKLASSIFICERAD INFORMATION

Republiken Finlands regering och Republiken Kroatiens regering (nedan ”parterna”), som

beaktar att parterna samarbetar bland annat, men inte enbart, i utrikes-, försvars-, säkerhets- och polisfrågor samt i vetenskaps-, näringslivs- och teknologifrågor,

inser att ett gott samarbete kan kräva utbyte av säkerhetsklassificerad information mellan parterna,

önskar bygga upp ett regelverk för att reglera det ömsesidiga skyddet av sådan säkerhetsklassificerad information som framställs eller utbyts mellan parterna eller mellan offentlig- eller privaträttsliga juridiska eller fysiska personer inom parternas jurisdiktion,

har kommit överens om följande:

Artikel 1

Mål

Målet med denna överenskommelse är att säkerställa skyddet av sådan säkerhetsklassificerad information som framställs eller utbyts allmänt mellan parterna.

Artikel 2

Definitioner

I denna överenskommelse avses med

(1) **”säkerhetsklassificerad information”** all information, oavsett form, som ska skyddas mot dataskyddskränkningar och som har

AGREEMENT BETWEEN THE GOVERNMENT OF THE REPUBLIC OF FINLAND AND THE GOVERNMENT OF THE REPUBLIC OF CROATIA ON MUTUAL PROTECTION OF CLASSIFIED INFORMATION

The Government of the Republic of Finland and the Government of the Republic of Croatia (hereinafter referred to as “the Parties”),

Considering that the Parties co-operate in matters such as, but not limited to, foreign affairs, defence, security, police, and science, industry and technology,

Realizing that good co-operation may require the exchange of Classified Information between the Parties,

Desiring to establish a set of rules regulating the mutual protection of Classified Information generated or exchanged between the Parties, or public or private legal entities or individuals under the jurisdiction of the Parties,

Have agreed as follows:

Article 1

Objective

The objective of this Agreement is to ensure the protection of Classified Information that is commonly generated or exchanged between the Parties.

Article 2

Definitions

For the purposes of this Agreement:

(1) **“Classified Information”** means any information, irrespective of form, which requires protection against Security Breach and

klassificerats i enlighet med den utlämnande partens nationella lagar och bestämmelser,

(2) **”informationsbehov”** behov av tillgång till säkerhetsklassificerad information i en bestämd officiell position och för att uträtta en bestämd uppgift,

(3) **”kränkning av dataskyddet”** alla former av röjande, ändring, missbruk, skadande eller förstörande av säkerhetsklassificerad information utan tillåtelse eller andra sådana handlingar eller försummelser som kan leda till att informationens sekretess, integritet eller användbarhet går förlorad,

(4) **”säkerhetsklass”** en kategori som i enlighet med nationella lagar och bestämmelser uttrycker hur begränsad tillgången till den säkerhetsklassificerade informationen är samt parternas minimiskyddsnivå för denna information,

(5) **”utlämnande part”** den part som lämnar ut säkerhetsklassificerad information eller under vilken säkerhetsklassificerad information framställs,

(6) **”mottagande part”** den part och offentlig- eller privaträttsliga juridiska eller fysiska personer inom partens jurisdiktion till vilken den utlämnande partens säkerhetsklassificerade information lämnas ut,

(7) **”nationell säkerhetsmyndighet”** den nationella myndighet som ansvarar för genomförandet och övervakningen av denna överenskommelse,

(8) **”behörig säkerhetsmyndighet”** en nationell säkerhetsmyndighet, en utsedd säkerhetsmyndighet eller en nationell informationssäkerhetsmyndighet eller någon annan nationell myndighet som i enlighet med nationella lagar och bestämmelser genomför denna överenskommelse,

(9) **”kontraktspart”** en fysisk eller juridisk person med rättskapacitet att ingå kontrakt,

(10) **”säkerhetsklassificerat kontrakt”** en överenskommelse mellan två eller flera kontraktsparter som inbegriper eller vars genomförande kräver tillgång till säkerhetsklassificerad information,

(11) **”säkerhetsutredning av person”** en bedömning i enlighet med nationella lagar och bestämmelser av den behöriga säkerhetsmyndigheten, enligt vilken en fysisk per-

has been classified in accordance with national laws and regulations of the Originating Party;

(2) **“Need-to-Know”** means the necessity to have access to Classified Information in the scope of a given official position and for the performance of a specific task;

(3) **“Security Breach”** means any form of unauthorized disclosure or alteration, misuse, damage or destruction of Classified Information, as well as any other action or inaction which may result in loss of its confidentiality, integrity or availability;

(4) **“Security Classification Level”** means a category which, in accordance with national laws and regulations, characterises the level of restriction of access to Classified Information and the minimum level of its protection by the Parties;

(5) **“Originating Party”** means the Party which provides Classified Information or under whose authority Classified Information is generated;

(6) **“Receiving Party”** means the Party, as well as any public or private legal entity or individual under its jurisdiction, to which Classified Information of the Originating Party is transmitted;

(7) **“National Security Authority”** means the national authority responsible for the implementation and supervision of this Agreement;

(8) **“Competent Security Authority”** means the National Security Authority, Designated Security Authority or National Communications Security Authority or another national authority which, in accordance with national laws and regulations, implements this Agreement;

(9) **“Contractor”** means an individual or a legal entity possessing the legal capacity to conclude contracts;

(10) **“Classified Contract”** means an agreement between two or more Contractors which involves or the execution of which requires access to Classified Information;

(11) **“Personnel Security Clearance”** means determination by the Competent Security Authority confirming, in accordance with its national laws and regulations, that an indi-

son kan beviljas tillgång till säkerhetsklassificerad information,

(12) **”säkerhetsutredning som gäller sammanslutning”** en bedömning av den behöriga säkerhetsmyndigheten som i enlighet med den berörda partens nationella lagar och bestämmelser bekräftar att en fysisk eller juridisk person uppfyller förutsättningarna för tillgång till och hantering av säkerhetsklassificerad information,

(13) **”tredje part”** en stat, organisation, juridisk eller fysisk person, som inte är part i denna överenskommelse.

vidual is eligible to have access to Classified Information;

(12) **“Facility Security Clearance**” means determination by the Competent Security Authority confirming, in accordance with its national laws and regulations, that a legal entity or individual meets the conditions for access to and handling of Classified Information;

(13) **“Third Party”** means any state, organization, legal entity or individual which is not a party to this Agreement.

Artikel 3

Säkerhetsklasser

1. Säkerhetsklassificerad information som lämnas ut i enlighet med denna överenskommelse ska förses med tillämplig anteckning om säkerhetsklass i enlighet med parternas nationella lagar och bestämmelser.

2. Parterna är överens om att följande säkerhetsklasser motsvarar varandra:

Article 3

Security Classification Levels

1. Any Classified Information provided under this Agreement shall be marked with the appropriate Security Classification Level in accordance with national laws and regulations of the Parties.

2. The Parties agree that the following Security Classification Levels are equivalent to each other:

Republiken Finland	Engelsk motsvarighet	Republiken Kroatien
ERITTÄIN SALAINEN eller YTTERST HEMLIG	TOP SECRET	VRLO TAJNO
SALAINEN eller HEMLIG	SECRET	TAJNO
LUOTTAMUKSELLINEN eller KONFIDENTIELL	CONFIDENTIAL	POVJERLJIVO
KÄYTTÖ RAJOITETTU eller BEGRÄNSAD TILLGÅNG	RESTRICTED	OGRANIČENO

For the Republic of Finland	Equivalent in English	For the Republic of Croatia
ERITTÄIN SALAINEN or YTTERST HEMLIG	TOP SECRET	VRLO TAJNO
SALAINEN or HEMLIG	SECRET	TAJNO

LUOTTAMUKSELLINEN or KONFIDENTIELL	CONFIDENTIAL	POVJERLJIVO
KÄYTTÖ RAJOITETTU or BEGRÄNSAD TILLGÅNG	RESTRICTED	OGRANIČENO

3. Den mottagande parten ska säkerställa att informationens säkerhetsklassificering inte ändras eller upphävs, utom med skriftligt tillstånd av den utlämnande parten.

Artikel 4

Behöriga säkerhetsmyndigheter

1. Parternas nationella säkerhetsmyndigheter är
I Republiken Finland
– utrikesministeriet,
I Republiken Kroatien
– Office of the National Security Council.
2. Parterna ska via diplomatiska kanaler underrätta varandra om eventuella ändringar som avser de nationella säkerhetsmyndigheterna. De nationella säkerhetsmyndigheterna ska underrätta varandra om eventuella andra behöriga säkerhetsmyndigheter och om senare ändringar som avser dem.
3. De nationella säkerhetsmyndigheterna ska underrätta varandra om gällande nationella lagar och bestämmelser som reglerar skyddet av säkerhetsklassificerad information och ska på begäran utbyta information angående säkerhetsstandarder, -förfaranden och -praxis för skyddet av säkerhetsklassificerad information.

Artikel 5

Skyddsåtgärder och tillgång till säkerhetsklassificerad information

1. Parterna vidtar alla lämpliga åtgärder i enlighet med sina nationella lagar och bestämmelser för att skydda säkerhetsklassificerad information som framställs eller utbyts i enlighet med denna överenskommelse. Sådan säkerhetsklassificerad information ska säkerställas ett skydd på samma nivå som nationell säkerhetsklassificerad information i motsva-

3. The Receiving Party shall ensure that the classifications of the information are not altered or revoked, except as authorised in writing by the Originating Party.

Article 4

Competent Security Authorities

1. The National Security Authorities of the Parties are:
For the Republic of Finland:
- Ministry for Foreign Affairs;
For the Republic of Croatia:
- Office of the National Security Council.
2. The Parties shall inform each other through diplomatic channels of any changes of the National Security Authorities. The National Security Authorities shall inform each other of any other Competent Security Authorities and any subsequent changes of these authorities.
3. The National Security Authorities shall inform each other of the national laws and regulations in force regulating the protection of Classified Information and shall, on request, exchange information about the security standards, procedures and practices for the protection of Classified Information.

Article 5

Protection Measures and Access to Classified Information

1. In accordance with their national laws and regulations, the Parties shall take all appropriate measures for the protection of Classified Information generated or exchanged under this Agreement. The same level of protection shall be ensured for such Classified Information as is provided to the national Classified Information of the equivalent Se-

rande säkerhetsklass enligt artikel 3.

2. Den utlämnande parten ska skriftligen underrätta den mottagande parten om ändringar i säkerhetsklassen för utlämnad säkerhetsklassificerad information för att den mottagande parten ska tillämpa lämpliga säkerhetsåtgärder.

3. Tillgång till säkerhetsklassificerad information ska endast beviljas fysiska personer som har ett informationsbehov, som har utfärdats en lämplig säkerhetsutredning av person i enlighet med nationella lagar och bestämmelser och som har fått instruktioner om sitt ansvar i skyddet av säkerhetsklassificerad information.

4. En säkerhetsutredning av person krävs inte för tillgång till säkerhetsklassificerad information i säkerhetsklass KÄYTTÖ RAJOITETTU eller BEGRÄNSAD TILLGÅNG / OGRANIČENO.

5. Inom räckvidden för denna överenskommelse erkänner bägge parter säkerhetsutredningar av personer eller sammanslutningar utfärdade av den andra parten.

6. De behöriga säkerhetsmyndigheterna bistår varandra på begäran och i enlighet med sina nationella lagar och bestämmelser med utredningsförfaranden som behövs för tillämpningen av denna överenskommelse.

7. Inom räckvidden för denna överenskommelse ska de nationella säkerhetsmyndigheterna utan dröjsmål underrätta varandra om ändringar i säkerhetsutredningar som avser personer eller sammanslutningar, i synnerhet vad gäller upphävande eller ändring av säkerhetsklasser.

8. På begäran av den utlämnande partens nationella säkerhetsmyndighet ska den mottagande partens nationella säkerhetsmyndighet ge en skriftlig bekräftelse på att en fysisk person har rätt att få tillgång till säkerhetsklassificerad information eller på att en juridisk person har utfärdats en säkerhetsutredning som gäller sammanslutning.

9. Den mottagande parten ska

a) förmedla säkerhetsklassificerad information till tredje parter endast med skriftligt förhandssamtycke av den utlämnande parten,

b) märka mottagen säkerhetsklassificerad information i enlighet med säkerhetsklass-

curity Classification Level, as defined in Article 3 of this Agreement.

2. The Originating Party shall inform the Receiving Party in writing about any change of the Security Classification Level of the released Classified Information, in order that the latter apply the appropriate security measures.

3. Access to Classified Information shall only be granted to individuals who have a Need-to-Know, who have been issued an appropriate Personnel Security Clearance in accordance with the national laws and regulations and who have been briefed on their responsibilities for the protection of Classified Information.

4. A Personnel Security Clearance is not required for access to Classified Information at the KÄYTTÖ RAJOITETTU or BEGRÄNSAD TILLGÅNG / OGRANIČENO level.

5. Within the scope of this Agreement, each Party shall recognize the Personnel and Facility Security Clearances issued by the other Party.

6. The Competent Security Authorities shall assist each other upon request and in accordance with their national laws and regulations in carrying out vetting procedures necessary for the application of this Agreement.

7. Within the scope of this Agreement, the National Security Authorities shall inform each other without delay about any alteration with regard to Personnel and Facility Security Clearances, in particular about the revocation or the alteration of Security Classification Levels.

8. Upon request of the National Security Authority of the Originating Party, the National Security Authority of the Receiving Party shall issue a written confirmation that an individual has the right to access Classified Information or a legal entity has been issued a Facility Security Clearance.

9. The Receiving Party shall:

a) submit Classified Information to a Third Party only upon prior written consent of the Originating Party;

b) mark the received Classified Information in accordance with the Security Classifica-

motsvarigheten i artikel 3,

c) använda säkerhetsklassificerad information endast för de ändamål den har utlämnats för.

10. Om det i någon annan överenskommelse mellan parterna förekommer strängare bestämmelser om utbyte eller skydd av säkerhetsklassificerad information, ska dessa strängare bestämmelser tillämpas.

Artikel 6

Förmedling av säkerhetsklassificerad information

1. Säkerhetsklassificerad information förmedlas via kanaler som de behöriga säkerhetsmyndigheterna sinsemellan har godkänt. Den mottagande parten ska bekräfta mottagandet av säkerhetsklassificerad information i säkerhetsklass SALAINEN eller HEMLIG / TAJNO och högre. Mottagandet av annan säkerhetsklassificerad information bekräftas på begäran.

2. Säkerhetsklassificerad information förmedlas elektroniskt endast på ett sådant säkert sätt som de behöriga säkerhetsmyndigheterna sinsemellan har kommit överens om.

Artikel 7

Kopiering och översättning av säkerhetsklassificerad information

1. Information i säkerhetsklass ERITTÄIN SALAINEN eller YTTERST HEMLIG / VRLO TAJNO översätts eller kopieras endast i undantagsfall, med den utlämnande partens skriftliga förhandssamtycke.

2. Alla kopior av säkerhetsklassificerad information ska förses med den ursprungliga klassificeringsanteckningen. Sådan kopierad information ska skyddas på samma sätt som den ursprungliga informationen. Antalet kopior ska begränsas till vad det officiella syftet kräver.

3. Översättningar av säkerhetsklassificerad information ska förses med samma klassificeringsanteckning som originalet och dessutom förses med en anmärkning på översättningstion Level equivalence set forth in Article 3;

c) use Classified Information only for the purposes that it has been provided for.

10. If any other agreement concluded between the Parties contains stricter regulations regarding the exchange or protection of Classified Information, these stricter regulations shall apply.

Article 6

Transmission of Classified Information

1. Classified Information shall be transmitted through channels mutually approved by the Competent Security Authorities. The Receiving Party shall confirm the receipt of Classified Information at the levels SALAINEN or HEMLIG / TAJNO and above. The receipt of other Classified Information shall be confirmed on request.

2. Classified Information shall be transmitted electronically only by secure means agreed between the Competent Security Authorities.

Article 7

Reproduction and Translation of Classified Information

1. Information classified at the ERITTÄIN SALAINEN or YTTERST HEMLIG / VRLO TAJNO level shall be translated or reproduced only in exceptional cases upon prior written consent of the Originating Party.

2. All copies of Classified Information shall be marked with the original classification marking. Such reproduced information shall be protected in the same way as the original information. The number of copies shall be limited to that required for official purposes.

3. Any translation of Classified Information shall be marked with the original classification marking and bear an additional note in the language of translation that the transla-

språket om att översättningen innehåller säkerhetsklassificerad information från den utlämnande parten.

Artikel 8

Utplåning av säkerhetsklassificerad information

1. Säkerhetsklassificerad information ska utplånas i syfte att förhindra att den helt eller delvis framställs på nytt.
2. Information i säkerhetsklass ERITTÄIN SALAINEN eller YTTERST HEMLIG / VRLO TAJNO utplånas inte. Den ska återlämnas till den utlämnande parten.
3. Den utlämnande parten kan med en tilläggsanteckning eller genom ett senare skriftligt meddelande uttryckligen förbjuda utplåning av säkerhetsklassificerad information. Om utplåning av säkerhetsklassificerad information förbjuds, ska informationen återlämnas till den utlämnande parten.
4. I krissituationer som gör det omöjligt att skydda eller återlämna säkerhetsklassificerad information som framställts eller utbytts i enlighet med denna överenskommelse ska den säkerhetsklassificerade informationen omedelbart utplånas. Den mottagande parten ska så fort som möjligt underrätta den utlämnande partens nationella säkerhetsmyndighet om att informationen har utplånats.

Artikel 9

Säkerhetsklassificerade kontrakt

1. Säkerhetsklassificerade kontrakt ingås och verkställs i enlighet med bägge parters nationella lagar och bestämmelser.
2. På begäran ska den mottagande partens nationella säkerhetsmyndighet bekräfta att en föreslagen kontraktspart har utfärdats en lämplig säkerhetsutredning av person eller sammanslutning. Om den föreslagna kontraktsparten inte har någon lämplig säkerhetsutredning, kan den utlämnande partens nationella säkerhetsmyndighet begära att den mottagande partens nationella säkerhetsmyndighet utfärdar en sådan.

tion contains Classified Information of the Originating Party.

Article 8

Destruction of Classified Information

1. Classified Information shall be destroyed insofar as to prevent its reconstruction in whole or in part.
2. Classified information at the ERITTÄIN SALAINEN or YTTERST HEMLIG / VRLO TAJNO level shall not be destroyed. It shall be returned to the Originating Party.
3. The Originating Party may, by additional marking or subsequent written notice, expressly prohibit the destruction of Classified Information. If the destruction of Classified Information is prohibited, it shall be returned to the Originating Party.

4. In case of a crisis situation which makes it impossible to protect or return Classified Information generated or exchanged under this Agreement the Classified Information shall be destroyed immediately. The Receiving Party shall notify the National Security Authority of the Originating Party about this destruction as soon as possible.

Article 9

Classified Contracts

1. Classified Contracts shall be concluded and implemented in accordance with national laws and regulations of each Party.

2. Upon request the National Security Authority of the Receiving Party shall confirm that a proposed Contractor has been issued an appropriate Personnel or Facility Security Clearance. If the proposed Contractor does not hold an appropriate security clearance, the National Security Authority of the Originating Party may request the National Security Authority of the Receiving Party to issue the appropriate security clearance.

3. För säkerhetsklassificerade kontrakt i säkerhetsklassen KÄYTTÖ RAJOITETTU eller BEGRÄNSAD TILLGÅNG / OGRANIČENO krävs ingen säkerhetsutredning som gäller sammanslutning.

4. Varje säkerhetsklassificerat kontrakt eller underleverantörskontrakt ska inkludera säkerhetsbestämmelser, där den utlämnande parten specificerar den säkerhetsklassificerade information som utlämnas till den mottagande parten, informationens säkerhetsklass samt kontraktspartens skyldigheter med avseende på skyddet av den säkerhetsklassificerade informationen.

5. En kontraktsparts skyldighet att skydda säkerhetsklassificerad information innefattar åtminstone följande:

a) att medge tillgång till säkerhetsklassificerad information i enlighet med nationella lagar och bestämmelser och med denna överenskommelse,

b) att förmedla den säkerhetsklassificerade informationen på det sätt som fastställts i denna överenskommelse,

c) att meddela om eventuella ändringar som avser den säkerhetsklassificerade informationen,

d) att använda säkerhetsklassificerad information som ingår i det säkerhetsklassificerade kontraktet endast för ändamål relaterade till kontraktets tema,

e) att noggrant följa bestämmelserna i denna överenskommelse med avseende på förfarandet vid hantering av säkerhetsklassificerad information,

f) att underrätta kontraktspartens nationella säkerhetsmyndighet om eventuella kränkningar av dataskyddet som rör den säkerhetsklassificerade informationen,

g) att till tredje parter lämna ut säkerhetsklassificerad information som anknyter till det säkerhetsklassificerade kontraktet endast med skriftligt förhandssamtycke av den utlämnande parten.

6. Underleverantörer som deltar i verkställandet av säkerhetsklassificerade kontrakt ska i tillämpliga fall följa de säkerhetsbestämmelser som tillämpas på kontraktsparter.

3. A Facility Security Clearance is not required for Classified Contracts at the KÄYTTÖ RAJOITETTU or BEGRÄNSAD TILLGÅNG / OGRANIČENO level.

4. Each Classified Contract or sub-contract shall include security provisions by which the Originating Party shall specify the Classified Information to be released to the Receiving Party, the Security Classification Level assigned to that information, and the Contractor's obligations to protect the Classified Information.

5. The Contractor's obligations to protect Classified Information shall include, at least, the following:

a) to grant access to the Classified Information in accordance with the national laws and regulations and this Agreement;

b) to transmit the Classified Information by the means specified in this Agreement;

c) to communicate any changes that may arise in respect of the Classified Information;

d) to use the Classified Information under the Classified Contract only for the purposes related to the subject of the contract;

e) to adhere strictly to the provisions of this Agreement related to the procedures for handling Classified Information;

f) to notify the Contractor's National Security Authority of any Security Breach related to the Classified Contract;

g) to release the Classified Information related to the Classified Contract to any Third Party only upon prior written consent of the Originating Party.

6. Sub-contractors engaged in Classified Contracts shall, as appropriate, comply with the security provisions applied to the Contractors.

Artikel 10

Besök

1. Besök som omfattar tillgång till säkerhetsklassificerad information kräver förhandstillstånd av värdpartens nationella säkerhetsmyndighet. Tillståndet beviljas utifrån en besöksbegäran av den besökande partens nationella säkerhetsmyndighet.

2. Den begäran som avses i punkt 1 i denna artikel ska innehålla

a) besökarens för- och efternamn, födelsedatum och födelseort samt nationalitet,

b) besökarens passnummer eller nummer på annat identitetsbevis,

c) besökarens ställning och namnet på den organisation besökaren representerar,

d) nivån på besökarens säkerhetsutredning av person,

e) besökets syfte och det föreslagna arbetsprogrammet, däribland den högsta säkerhetsklassen för säkerhetsklassificerad information besöket inbegriper, samt planerad tidpunkt för besöket,

f) namnen på organisationer och arbetsställen besöket avser,

g) besökens antal och längd,

h) eventuella andra uppgifter som de nationella säkerhetsmyndigheterna sinsemellan kommer överens om.

3. Begäran som avses i punkt 1 i denna artikel ska framföras minst tre veckor i förväg. I brådskande fall får de behöriga säkerhetsmyndigheterna komma överens om en kortare tidsfrist.

4. Vardera parten garanterar skyddet av besökarnas personuppgifter i enlighet med sina nationella lagar och bestämmelser.

Artikel 11

Kränkning av dataskyddet

1. När en kränkning av dataskyddet har skett ska den partens nationella säkerhetsmyndighet, inom vars territorium kränkningen har skett, utan dröjsmål underrätta den utlämnande partens nationella säkerhetsmyndighet om kränkningen och inleda ett lämpligt förfarande i enlighet med sina nationella

Article 10

Visits

1. Visits entailing access to Classified Information are subject to prior permission by the National Security Authority of the host Party. The permission shall be granted on the basis of a visit request by the National Security Authority of the visiting Party.

2. The request referred to in paragraph 1 of this Article shall contain:

a) the visitor's name and surname, date and place of birth, and nationality;

b) the passport number or another identification card number of the visitor;

c) the position of the visitor and the name of the organization represented;

d) the level of the Personnel Security Clearance of the visitor;

e) the purpose, proposed working programme, including the highest level of Classified Information involved, and planned date of the visit;

f) the names of the organizations and facilities requested to be visited;

g) the number of visits and the period required;

h) any other data, agreed upon by the National Security Authorities.

3. The request referred to in paragraph 1 of this Article shall be submitted at least 3 weeks in advance. In urgent cases the National Security Authorities may agree on a shorter period.

4. Each Party shall guarantee the protection of the personal data of the visitors in accordance with its national laws and regulations.

Article 11

Security Breach

1. In case of a Security Breach, the National Security Authority of the Party where the breach has occurred shall, without delay, inform the National Security Authority of the Originating Party about the breach and, in accordance with national laws and regulations, initiate appropriate proceedings in or-

lagar och bestämmelser för att fastställa omständigheterna kring kränkningen. Resultatet av förfarandet ska lämnas till den utlämnande partens nationella säkerhetsmyndighet.

2. När en kränkning av dataskyddet sker i en tredje stat ska den nationella säkerhetsmyndigheten hos den sändande parten utan dröjsmål vidta åtgärder enligt punkt 1 i denna artikel.

Artikel 12

Kostnader

Vardera parten står för sina egna kostnader som genomförandet och övervakningen av denna överenskommelse medför.

Artikel 13

Tvistlösning

Alla tvister om tolkningen eller tillämpningen av denna överenskommelse ska avgöras genom samråd och förhandlingar mellan parterna och inte hänskjutas till någon internationell domstol eller tredje part för avgörande.

Artikel 14

Slutbestämmelser

1. Denna överenskommelse träder i kraft den första dagen i den andra månaden efter att den senare skriftliga underrättelsen har mottagits där parterna via diplomatiska kanaler meddelar varandra att de nationella rättsliga kraven som ikraftträdandet av överenskommelsen förutsätter har uppfyllts.

2. Denna överenskommelse kan ändras på gemensam skriftlig överenskommelse mellan parterna. Ändringarna träder i kraft i enlighet med punkt 1 i denna artikel.

3. Denna överenskommelse gäller tills vidare. Vardera parten får säga upp överenskommelsen genom skriftlig anmälan till den andra parten via diplomatiska kanaler. I det fallet upphör överenskommelsen att gälla sex månader från den dag, då den andra parten mot-

der to determine the circumstances of the Security Breach. The results of the proceedings shall be forwarded to the National Security Authority of the Originating Party.

2. When the Security Breach has occurred in a third state, the National Security Authority of the sending Party shall take the actions referred to in paragraph 1 of this Article without delay.

Article 12

Expenses

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

Article 13

Settlement of Disputes

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

Article 14

Final Provisions

1. This Agreement shall enter into force on the first day of the second month following the receipt of the last written notification by which the Parties have informed each other, through diplomatic channels, that their internal legal requirements necessary for the entry into force of the Agreement have been fulfilled.

2. This Agreement may be amended by mutual written consent of the Parties. The amendments shall enter into force in accordance with the provision of paragraph 1 of this Article.

3. This Agreement is concluded for an indefinite period of time. Either Party may denounce this Agreement by giving the other Party written notice through diplomatic channels. In that case, this Agreement shall

tog anmälan om uppsägning.

4. Om denna överenskommelse upphör att gälla, ska all säkerhetsklassificerad information som har utbytts i enlighet med överenskommelsen fortsatt skyddas i enlighet med bestämmelserna i överenskommelsen och på begäran ska denna information återlämnas till den utlämnande parten.

Upprättad i Zagreb den 11 februari 2014 i två originalexemplar på finska, kroatiska och engelska, där alla texter är lika giltiga I händelse av tolkningsskiljaktighet ska den engelska texten gälla.

För Republiken Finlands regering

Timo Rajakangas
Ambassadör

För Republiken Kroatiens regering

Ivica Panenic
Chef för nationella säkerhetsmyndighetens byrå

terminate six months from the date on which the other Party has received the denunciation notice.

4. In case of termination of this Agreement, all Classified Information exchanged pursuant to this Agreement shall continue to be protected in accordance with the provisions set forth herein and, upon request, returned to the Originating Party.

Done at Zagreb on 11th February in two originals, each in the Finnish, Croatian and English languages, all texts being equally authentic. In case of any divergence of interpretation, the English text shall prevail.

For the Government of the Republic of Finland

Timo Rajakangas
Ambassador

For the Government of the Republic of Croatia Kroatian tasavallan hallituksen puolesta

Ivica Panenic
Head of the Office of the National Security Council