

Regeringens proposition till riksdagen om godkännande av överenskommelsen mellan Finland och Schweiz 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 propositionen föreslås att riksdagen ska godkänna överenskommelsen mellan Finland och Schweiz 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 Schweiz i samarbetet mellan parterna särskilt i frågor som rör utrikesärenden, försvar, säkerhet, vetenskap, företag eller teknik. 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 när den senare underrättelsen har tagits emot om att de nationella åtgärder som krävs för ikraftträdandet av överenskommelsen har slutförts. Lagen om sättande i kraft av överenskommelsen avses träda i kraft samtidigt som överenskommelsen träder i kraft för Finlands del, vid en tidpunkt som bestäms genom förordning av statsrådet.

INNEHÅLL

PROPOSITIONENS HUVUDSAKLIGA INNEHÅLL	1
INNEHÅLL	2
ALLMÄN MOTIVERING	3
1 INLEDNING	3
2 NULÄGE	4
2.1 Lagen om internationella förpliktelser som gäller informationssäkerhet	4
2.2 Lagstiftningen om säkerhetsutredningar	8
3 MÅLSÄTTNING OCH DE VIKTIGASTE FÖRSLAGEN	8
4 PROPOSITIONENS KONSEKVENSER	8
4.1 Konsekvenser för medborgarna	8
4.2 Konsekvenser för näringslivet	9
4.3 Ekonomiska konsekvenser	9
4.4 Konsekvenser för förvaltningen	9
5 BEREDNINGEN AV PROPOSITIONEN	10
DETALJMOTIVERING	11
1 Överenskommelsens innehåll och förhållande till lagstiftningen i Finland	11
2 Lagförslag	15
3 Ikraftträdande	16
4 Behovet av riksdagens samtycke och behandlingsordning	16
4.1 Behovet av riksdagens samtycke	16
4.2 Behandlingsordning	17
LAGFÖRSLAG	19
Lag om sättande i kraft av de bestämmelser som hör till området för lagstiftningen i överenskommelsen med Schweiz om ömsesidigt skydd av säkerhetsklassificerad information	19
FÖRDRAGSTEXT	20
BILAGA 1	30
BILAGA 2	31

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 lokalernas 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 vid 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 utgör det generella säkerhetsskyddsavtalet om ömsesidigt skydd och utbyte av säkerhetsskyddsklassificerade uppgifter mellan Danmark, Finland, Island, Norge och Sverige (FördrS 11 och 12/2013).

I avsaknad av en konvention har staterna, Finland medräknat, varit tvungna att lösa frågan genom bilaterala överenskommelser. Finland ingick sin första bilaterala överenskommelse om informationssäkerhet med Tyska förbundsrepubliken år 2004. Den trädde i kraft den 16 juli 2004 (FördrS 96 och 97/2004). Ett år senare undertecknades en överenskommelse mellan Finland och Frankrike och den i sin tur trädde 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 ekonomisk växelverkan. Det faktum att behovet av informationssäkerhet i allt högre grad börjar fokusera också på ekonomisk verksamhet kommer till uttryck i samarbetsavtalet mellan Finland och Europeiska rymdorganisationen (ESA), nedan *ESA-överenskommelsen*, även den från 2004 (FördrS 94 och 95/2004). En av de viktigaste målsättningarna med överenskommelsen har varit att säkerställa det finska näringslivets möjligheter att på jämlik grund med de andra medlemsländerna kunna delta i ESA:s säkerhetsklassificerade anbuds förfaranden. Finland 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) och Luxemburg (FördrS 59 och 60/2013). Den 10 maj 2012 godkände Finland det i maj 2011 undertecknade avtalet mellan EU:s medlemsstater om skydd av säkerhetsskyddsklassificerade uppgifter, men avtalet har hittills inte trätt i kraft. 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 informations-säkerhet skapas förutsättningar för utbyte av säkerhetsklassificerad information mellan parterna. Genom överenskommelsen säkerställs att säkerhetsklassificerad information som Finland lämnar ut hålls hemlig i mottagarstaten och skyddas och hanteras på ett korrekt sätt. Med hjälp av 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 även efter att den utlämnats hos den utlämnande staten. 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 ytterligare handlingar som har upprättats av en finsk myndighet eller av en näringsidkare som hör till lagens tillämpningsområde, av vilka 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 utifrån särskilt känsligt informationsmaterial. Lagen tillämpas inte endast för hemlighållande eller klassificering av handlingar och delar av handlingar som innehåller nationell information från Finland.

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

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 en näringsidkare och dennes anställda i sådana fall då näringsidkaren är part i ett säkerhetsklassificerat avtal eller deltar i ett upphandlingsförfarande innan ett sådant avtal ingås eller är underleverantör för en sådan näringsidkare (1 § 2 mom.).

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

För att kunna delta i ett anbuds-förfarande som ordnas av en myndighet i en annan stat eller av ett företag som har hemvist i den andra staten kan en näringsidkare begära att det görs en säkerhetsutredning som gäller sammanslutningar samt en bedömning (12 § 2 mom.). Syftet med bestämmelsen är att säkerställa finländska företags möjligheter att konkurrera om upphandlingar också när det inte finns någon internationell överenskommelse om informationssäkerhet som kan tillämpas på upphandlingen. De flesta stater förutsätter dock att det finns en bilateral överenskommelse om informationssäkerhet

förrän de godkänner ett utländskt säkerhetsintyg.

En näringsidkare och den som är anställd av eller handlar på uppdrag av en näringsidkare har sekretessplikt i fråga om särskilt känsligt informationsmaterial (6 §). 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 i samband med anbuds- och upphandlingsförfaranden.

Skyddspolisen och huvudstaben svarar för utredningar som gäller personsäkerhet, nedan personsäkerhetsutredning, (11 §). Enligt lagen hör säkerhetsutredningar som gäller sammanslutningar till Skyddspolisen, utom då det är fråga om anskaffningar som hänför sig till försvaret, då utredningen utförs av huvudstaben (12 §). Enligt 5 § 2 mom. i lagen om internationella förpliktelser som gäller informationssäkerhet kan den nationella säkerhetsmyndigheten och de utsedda säkerhetsmyndigheterna, oavsett vad som föreskrivs om behörighet att göra säkerhetsutredningar som gäller sammanslutningar, 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 informationssäkerhet (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. Enligt 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 informationsmaterial som dess säkerhetsklass förutsätter samt ett bemyndigande att genom förordning av statsrådet föreskriva om sådana säkerhetsåtgärder vid hantering av särskilt känsligt informationsmaterial som svarar mot olika säkerhetsklasser (9 §). I 11 § i statsrådets förordning om informationssäkerheten inom statsförvaltningen (681/2010), här efter *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

Personsäkerhetsutredningar som förutsätts i internationella förpliktelser om informations-säkerhet ska göras så som föreskrivs i och med stöd av lagen om säkerhetsutredningar (177/2002). Till exempel den personens rättigheter som är föremål för utredningen fastställs alltså enligt den lagen.

I lagen om internationella förpliktelser som gäller informationssäkerhet ingår emellertid två bestämmelser som är specialbestämmelser i förhållande till lagen om säkerhetsutredningar. En begränsad säkerhetsutredning kan göras också i andra fall än de som räknas upp i 19 § i lagen om säkerhetsutredningar, om en sådan är nödvändig för att uppfylla den internationella förpliktelser om informationssäkerhet (11 § 1 mom.). Den andra specialbestämmelsen reglerar myndigheternas befogenheter. Säkerhetsutredningen ska göras av huvudstaben då en sådan behövs för att uppfylla en internationell förpliktelse som gäller försvarsförvaltningen eller anskaffningar av försvarsmateriel. I övriga fall görs utredningar som hänför sig till personsäkerhet av Skyddspolisen (11 § 2 mom.). Enligt 10 § 2 mom. i lagen om säkerhetsutredningar får den behöriga myndighetens bedömning av tillförlitligheten eller lämpligheten för en tjänst eller ett uppdrag hos den som utredningen gäller inte ingå i en säkerhetsutredning, om inte ett fördrag eller någon annan internationell förpliktelse som avses i lagens 9 § förutsätter det. Eftersom huvudregeln är att en säkerhetsutredning inte 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 överenskommit 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 överlä-

tande av intyget till den berörda personen själv (14 §).

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 lokaler och hanteringskutymmer 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 ut 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 en del av 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).

2.2 Lagstiftningen om säkerhetsutredningar

Bestämmelser om personsäkerhetsutredningar 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 uppräkningslista över de register som får användas vid utredningsförfarandet.

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

Den arbetsgrupp som justitieministeriet hade tillsatt för en översyn av lagen om säkerhetsutredningar överlätt sitt betänkande till justitieministern den 31 januari 2011. Arbetsgruppen hade i uppdrag att utveckla lagen om säkerhetsutredningar så att den stämmer överens med de skyldigheter som är bindande för Finland och med allmän internationell praxis. Regeringens proposition till riksdagen med förslag till säkerhetsutredningslag och lagar som har samband med den (RP 57/2013 rd) överlämnades till riksdagen under vårsessionsperioden och propositionen är ännu inte slutbehandlad. Propositionen om säkerhetsutredningslagen, om den godkänns, inverkar inte på de bestämmelser i överenskommelsen som här föreläggs för godkännande.

3 Målsättning och de viktigaste förslagen

Syftet med propositionen är att sätta i kraft överenskommelsen om informationssäkerhet mellan Finland och Schweiz och säkerställa att säkerhetsklassificerad information som Finland lämnar ut till Schweiz skyddas och hanteras på ett korrekt sätt. Propositionen syftar också till att främja Finlands möjligheter att ta emot säkerhetsklassificerad information från Schweiz och så förbättra samarbetet mellan länderna inom informationssäkerhetsområdet. Ytterligare syftar propositionen till att trygga finländska företags möjligheter att delta i internationella projekt eller projekt mellan Finland och Schweiz som kan kräva utbyte av säkerhetsklassificerad information och på det sättet förbättra de finländska företagens konkurrenskraft.

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 Schweiz 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 Schweiz gäller handlingar som Schweiz anser att ska vara sekretessbelagda och följaktligen har försett med hög säkerhetsklassificering. I artikel 5 i överenskommelsen föreskrivs om sekretessen med avseende på säkerhetsklassificerad information. Enligt punkt 2 i artikeln ger parterna inte tredje parter tillgång till säkerhetsklassificerad information utan den utlämnande partens skriftliga förhandssamtycke. 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 Schweiz 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 Schweiz 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 säkerhetsut-

redningar 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 Schweiz. Analogt öppnar överenskommelsen möjligheter för schweiziska 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 schweiziska 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. Utlåtanden om propositionen har begärts av justitieministeriet, försvarsministeriet, inri-

kesministeriet, finansministeriet, kommunikationsministeriet, arbets- och näringsministeriet, Skyddspolisen och Kommunikationsverket. Utlåtanden har lämnats av arbets- och näringsministeriet, försvarsministeriet, inrikesministeriet och kommunikationsministeriet. Utlåtandena förordar att avtalet godkänns och sätts i kraft.

DETALJMOTIVERING

1 Överenskommelsens innehåll och förhållande till lagstiftningen i Finland

Artikel 1. Överenskommelsens syfte och tillämpningsområde. I artikeln definieras att syftet med överenskommelsen är att säkerställa skyddet av sådan säkerhetsklassificerad information som utbyts eller framställs i samarbetet mellan Finland och Schweiz. I inledningen till överenskommelsen anges att parternas samarbetsområden omfattar frågor som rör utrikesärenden, försvar, säkerhet, vetenskap, företag eller teknik.

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

I punkt a definieras säkerhetsklassificerad information. Överenskommelsen gäller handlingar eller material, oavsett form, karaktär eller förmedlingssätt som en part lämnar ut till den andra parten och som har säkerhetsklassificerats och försetts med relevant anteckning om säkerhetsklass i enlighet med nationella lagar och bestämmelser. Överenskommelsen omfattar också information, handlingar eller material som framställs utgående från sådan säkerhetsklassificerad information och som har försetts med relevant anteckning om säkerhetsklass. Punkten är i samklang med 2 § 1 mom. i lagen om internationella förpliktelser som gäller informationssäkerhet.

Enligt punkt b avses med säkerhetsklassificerat kontrakt ett kontrakt eller underleverantörskontrakt, inbegripet förhandlingar som föregår kontrakt, som innehåller eller som har anknytning till säkerhetsklassificerad information. Punkten är i samklang med 2 § 3 mom. i lagen om internationella förpliktelser som gäller informationssäkerhet.

Enligt punkt c avses med utlämnande part den part som lämnar ut säkerhetsklassificerad information. Definitionen omfattar också offentlig- eller privaträttsliga juridiska och fysiska personer inom partens jurisdiktion.

Enligt punkt d avses med mottagande part den part till vilken den utlämnande parten lämnar ut säkerhetsklassificerad information. Definitionen omfattar också offentlig- eller

privaträttsliga juridiska och fysiska personer inom partens jurisdiktion.

Enligt punkt e avses med behörig säkerhetsmyndighet en nationell säkerhetsmyndighet, en utsedd säkerhetsmyndighet eller ett annat behörigt organ som i enlighet med nationella lagar och bestämmelser har beordrigats att ansvara för genomförandet av överenskommelsen. Enligt lagen om internationella förpliktelser som gäller informationssäkerhet är denna myndighet i Finland utrikesministeriet, där uppgiften sköts av Nationella säkerhetsmyndigheten. Härutöver är försvarsministeriet, huvudstaben, Skyddspolis och Kommunikationsverket utsedda säkerhetsmyndigheter.

I punkt f definieras kränkning av dataskyddet som en gärning eller försummelse som bryter mot nationella lagar och bestämmelser och som kan medföra att säkerhetsklassificerade uppgifter försvinner eller äventyras.

I punkt g definieras begreppet säkerhetsutredning som ett positivt utfall av en prövning, baserad på nationella lagar och bestämmelser, av lämpligheten hos en juridisk eller fysisk person för tillgång till och hantering av säkerhetsklassificerade uppgifter på en bestämd nivå.

Artikel 3. 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). Till nationell säkerhetsmyndighet i Schweiz har utsetts försvarsministeriet där uppgiften sköts av avdelningen för informations- och fastighetssäkerhet (Directorate for Information Security and Facility Protection, IOS).

I punkt 2 förpliktas parterna att underrätta varandra om andra behöriga säkerhetsmyndigheter (Competent Security Authorities, CSA) som ansvarar för genomförandet av olika delar av överenskommelsen. Utsedda säkerhetsmyndigheter (Designated Security Authority, DSA) i Finland är enligt 4 § i la-

gen om internationella förpliktelser som gäller informationssäkerhet försvarsministeriet, huvudstaben, Skyddspolisen och Kommunikationsverket.

I punkt 3 förpliktas parterna att underrätta varandra om eventuella senare ändringar i de behöriga säkerhetsmyndigheterna.

Artikel 4. 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 Schweiz säkerhetsklasser motsvarar varandra. I Schweiz anges säkerhetsklassen aningen på tyska, franska eller italienska. Den högsta säkerhetsklassen, som kräver de strängaste informationssäkerhetsåtgärderna, är "ERITTÄIN SALAINEN/YTTERST HEMLIG". 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. Schweiz har ingen klass som motsvarar Finlands högsta säkerhetsklass. I punkt 5 i artikeln är utgångspunkten i stället att, om Finland skickar information till Schweiz i säkerhetsklass ERITTÄIN SALAINEN/YTTERST HEMLIG, de behöriga säkerhetsmyndigheterna separat ska komma överens om hur informationen ska hanteras. Den nästhögsta säkerhetsklassen är "SALAINEN/HEMLIG" (GEHEIM/SECRET/EGRETO). 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" (VERTRAULICH/KONFIDENTIEL/ KONFIDENZIALE), 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/EGRÄNSAD TILLGÅNG" (INTERN/INTERNE/AD USO INTERNO), 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 säkerhetsklass 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 tillgodo-seendet av internationella förpliktelser som gäller informationssäkerheten i 12 § i förordningen. I 11 § 1 mom. i förordningen föreskrivs om 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 tillgodo-seendet 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.

I punkt 3 i artikeln fastställs att de engelska beteckningarna TOP SECRET, SECRET, CONFIDENTIAL och RESTRICTED motsvarar de finländska och schweiziska termerna i tabellen.

Enligt punkt 4 ska den mottagande parten säkerställa att säkerhetsklasser inte ändras eller upphävs utan skriftligt tillstånd av den utlämnande parten.

Artikel 5. Skydd av säkerhetsklassificerad information. Artikeln innehåller de viktigaste förpliktelserna om ömsesidigt skydd.

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

I punkt 2 förbjuds utlämnande av säkerhetsklassificerad information till tredje parter utan skriftligt förhandssamtycke av den utlämnande parten. Punkten förpliktar parterna att följa principen om utlämnarens samtycke.

Punkt 3 gäller personalsäkerhet. Tillgång till säkerhetsklassificerad information ska enligt bestämmelsen endast beviljas personer som har ett informationsbehov, som har säkerhetsklarats enligt nationella lagar och bestämmelser och som har fått tillstånd att få tillgång till sådan information. Dessutom ska de få instruktioner om sitt ansvar i skyddet av informationen. Bestämmelsen är i samklang med 6 § 3 mom. i lagen om internationella förpliktelser som gäller informationssäkerhet, enligt vilken endast personer som behöver informationen för skötseln av sina uppgifter ska ha tillgång till materialet. Den kontroll av en persons tillförlitlighet som internationella informationssäkerhetsförpliktelser kräver ska i Finland utföras i enlighet med lagen om säkerhetsutredningar och med 11 § i lagen om internationella förpliktelser som gäller informationssäkerhet. Personssäkerhetsutredningar görs av huvudstaben i ärenden som gäller försvarsförvaltningen, i övriga fall av Skyddspolisén.

Enligt punkt 4 får säkerhetsklassificerad information endast användas för angivet ändamål. En bestämmelse som motsvarar förpliktelsen finns i 6 § 2 mom. i lagen om internationella förpliktelser om informationssäkerhet.

Artikel 6. Säkerhetsklassificerade kontrakt. Artikeln innehåller de bestämmelser som avses i artikel 2 led b om säkerhetsklassificerade kontrakt som ingås inom någondera partens territorium.

Enligt punkt 1 i artikeln ska den mottagande partens behöriga säkerhetsmyndighet på begäran meddela den utlämnande partens behöriga säkerhetsmyndighet huruvida den föreslagna kontraktsparten hos den mottagande parten har beviljats intyg över säkerhetsutredning i den säkerhetsklass som krävs (Facility Security Clearance, FSC). Har kontraktsparten i fråga inte det intyg över säkerhetsutredning som krävs, kan den utlämnande partens behöriga säkerhetsmyndighet be den mottagande partens behöriga säkerhetsmyndighet säkerhetsklara kontraktsparten.

Enligt punkt 2 kan mottagarpartens behöriga säkerhetsmyndighet vid öppna anbudsförfaranden även utan officiell begäran överlämna de relevanta intygen över säkerhetsutredningar till den utlämnande partens behöriga säkerhetsmyndighet.

I punkt 3 åläggs parterna att i säkerhetsklassificerade kontrakt inkludera relevanta säkerhetsbestämmelser, däribland klassificeringsanvisningar. En kopia av säkerhetsbestämmelserna ska skickas till den partens behöriga säkerhetsmyndigheter inom vars jurisdiktion det säkerhetsklassificerade kontraktet ska genomföras. Nationella bestämmelser om säkerhetsklassificerade kontrakt finns i 1 § 2 mom. (tillämpning 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. 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 4 får representanter för parternas behöriga säkerhetsmyndigheter besöka varandra för att analysera effekten av de åtgärder som en kontraktspart har vidtagit för att skydda säkerhetsklassificerad information

i anknytning till ett säkerhetsklassificerat kontrakt. Bestämmelsen har också samband med artikel 10.2 i överenskommelsen där det bestäms om besök av parternas säkerhetsmyndigheter.

Artikel 7. Förmedling och registrering av säkerhetsklassificerad information. Artikeln innehåller bestämmelserna om förfarandet vid överföring av säkerhetsklassificerad information mellan parterna.

Parterna ska enligt punkt 1 förmedla informationen med hjälp av skyddade mellanstatliga kanaler eller så som de behöriga säkerhetsmyndigheterna annars kommer överens om. Bestämmelsen är i samklang med 18 § i informationssäkerhetsförordningen om förmedling av en handling och med 19 § om överföring av en handling i datanätet. Enligt punkt 2 i artikeln ska information i säkerhetsklass LUOTTAMUKSELLINEN/ KONFIDENTIELL eller högre som utbyts mellan parterna registreras på ett lämpligt sätt och i enlighet med nationella lagar och bestämmelser. Bestämmelsen är i samklang med 20 § i informationssäkerhetsförordningen om dokumentation av hanteringen, enligt vilken hanteringen av handlingar som omfattas av skyddsnivå I–III ska dokumenteras i en elektronisk logg, ett datasystem, ett ärendehanteringssystem, ett manuellt diarium eller en handling.

Artikel 8. Översättning, kopiering och utplåning av säkerhetsklassificerad information. Artikeln innehåller bestämmelser om hur material i olika säkerhetsklasser får översättas, kopieras och utplånas.

I punkt 1 förpliktas parterna att förse alla översättningar och kopior av säkerhetsklassificerad information med samma anteckning om säkerhetsklass som originalet och att skydda dem i enlighet med det. Endast minimiantalet kopior som det officiella ändamålet kräver får tas.

I punkt 2 förpliktas parterna att förse alla översättningar med relevant anteckning på det översatta språket om att översättningen innehåller säkerhetsklassificerad information.

Enligt punkt 3 får information i säkerhetsklass SALAINEN/HEMLIG eller högre översättas eller kopieras endast med skriftligt samtycke av den utlämnande parten.

Enligt punkt 4 får information i säkerhetsklass SALAINEN/HEMLIG inte utplånas

utan skriftligt förhandssamtycke av den utlämnande parten. Informationen ska returneras till den utlämnande parten när parterna anser att den inte längre behövs.

Enligt punkt 5 ska information i säkerhetsklass LUOTTAMUKSELLINEN/KONFIDENTIELL utplånas när det anses att den inte längre behövs.

Punkt 6 innehåller en bestämmelse som gäller krissituationer. Bestämmelsen ålägger parterna att omedelbart utplåna säkerhetsklassificerad information som har lämnats ut i enlighet med överenskommelsen, om en krissituation hindrar att informationen skyddas. Den utlämnande partens behöriga säkerhetsmyndigheter ska så snart som möjligt underrättas om utplåningen.

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. Närmare bestämmelser om hanteringen regleras i Finland på förordningsnivå. I informationssäkerhetsförordningen som utfärdats med stöd av offentlighetslagen föreskrivs i 17 § om kopiering av handlingar och i 21 § om arkivering och förstöring av handlingar.

Artikel 9. Besök. Artikeln tillämpas på besök som omfattar tillgång till säkerhetsklassificerad information. Enligt punkt 1 behövs det ett skriftligt förhandstillstånd av värdpartens behöriga säkerhetsmyndighet för sådana besök. Besökare ska få tillgång till säkerhetsklassificerad information endast, om de har den sändande partens tillstånd för besöket (punkt a), de har fått ett relevant intyg över personsäkerhetsundersökning (punkt b), och de har fått tillstånd att ta emot säkerhetsklassificerad information i enlighet med värdpartens lagar och bestämmelser (punkt c).

Punkt 2 innehåller bestämmelser om de förfaranden som ska följas vid besök. Enligt tidsfristen som anges i stycket ska värdpartens behöriga säkerhetsmyndighet få begäran om besöket minst 14 dagar före den planerade tidpunkten för besöket. I brådskande fall kan de behöriga säkerhetsmyndigheterna komma överens om en kortare tidsfrist. Be-

söksbegäran ska innehålla de uppgifter som avses i bilaga 2 till denna överenskommelse.

Enligt punkt 3 är besökstillstånd giltiga i högst 12 månader.

Artikel 10. Säkerhetssamarbete. I punkt 1 förpliktas de behöriga säkerhetsmyndigheterna att informera varandra om sina relevanta nationella lagar och bestämmelser som gäller skyddet av säkerhetsklassificerad information, och om eventuella ändringar i dem.

Enligt punkt 2 ska de behöriga säkerhetsmyndigheterna för att säkerställa ett nära samarbete i verkställandet av överenskommelsen vid behov samråda och på begäran informera varandra om sina nationella säkerhetsnormer, förfaranden och tillämpningar för skyddet av säkerhetsklassificerad information. För att uppnå detta mål får de behöriga säkerhetsmyndigheterna besöka varandra. Bestämmelser om besök finns i 18 § i lagen om internationella förpliktelser som gäller informationssäkerhet.

Enligt punkt 3 ska de behöriga säkerhetsmyndigheterna i enlighet med parternas nationella lagar och bestämmelser på begäran bistå varandra med att utföra säkerhetsutredningar som gäller personer eller sammanslutningar.

Enligt punkt 4 ska de nationella säkerhetsmyndigheterna utan dröjsmål underrätta varandra om ändringar i de relevanta säkerhetsutredningarna.

I punkt 5 konstateras att överenskommelsen inte tillämpas på utbyte av säkerhetsklassificerad information mellan parternas underlättelsejänster eller brottsbekämpande myndigheter såsom polisen.

Artikel 11. Kränkning av dataskyddet. I punkt 1 förpliktas parterna att utan dröjsmål underrätta varandra om misstänkta eller upptäckta fall av kränkningar av dataskyddet.

Enligt punkt 2 åtar sig parterna att utan dröjsmål undersöka incidenter inom ramen för internationell rätt och sin nationella jurisdiktion. Den andra parten ska vid behov samarbeta med den behöriga parten i undersökningen. Enligt punkt 3 ska parterna inom ramen för internationell rätt och sin nationella jurisdiktion vidta alla relevanta åtgärder som är förenliga med nationella lagar och bestämmelser för att begränsa konsekvenserna av kränkningar av dataskyddet och för att fö-

rebygga ytterligare incidenter. Den andra parten ska underrättas om resultaten av undersökningen och vidtagna åtgärder. 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 de kostnader som förorsakas dem genom verkställandet av förpliktelserna i överenskommelsen.

Artikel 13. Tvistlösning. Enligt artikeln ska alla tvister mellan parterna angående tolkning eller tillämpning av överenskommelsen uteslutande avgöras i samråd mellan parterna.

Artikel 14. Slutbestämmelser. I artikeln ingår bestämmelser om ikraftträdandet, 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. En part kan säga upp överenskommelsen genom skriftlig anmälan till den andra parten via diplomatiska kanaler, iakttagande en uppsägningstid på sex månader.

I slutet av överenskommelsen konstateras det att den ersätter samarbetsprotokollet mellan Finlands försvarsministerium och schweiziska försvarsministeriet om utbyte av säkerhetsklassificerad information som undertecknades den 17 mars 1994 i Bern.

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 Schweiz, 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 Schweiz ska parterna underrätta varandra när de nationella förfaranden som krävs för ikraftträdandet av överenskommelsen har slutförts. Överenskommelsen träder i kraft den första dagen den andra månaden efter att den senare underrättelsen har tagits emot.

Lagen om sättande i kraft av överenskommelsen avses träda i kraft samtidigt som överenskommelsen träder i kraft för Finlands del, 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 anförts ovan krävs riksdagens samtycke för flera bestämmelser i överenskommelsen som ingår i propositionen. I artikel 2 definieras 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).

I artikel 3 ställs det fast att utrikesministeriet är Finlands nationella säkerhetsmyndighet. Bestämmelsen motsvarar 4 § 1 mom. i lagen om internationella förpliktelser som gäller informationssäkerhet. Bestämmelsen är konstaterande och ska därför inte anses förutsätta riksdagens samtycke.

Artikel 4 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 föras 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 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 informa-

tionen. Artikel 5 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 om parternas skyldighet att låta utföra en relevant 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 tryggt 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. Bestämmelsen hör följaktligen till området för lagstiftningen och kräver riksdagens samtycke för att träda i kraft. Enligt artikel 5.4 får säkerhetsklassificerad information endast användas för angivet ändamål. 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 6 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. Besök av parternas säkerhetsmyndigheter anknyter till artikel 6.4 där besöken av parternas behöriga säkerhetsmyndigheter möjliggörs. Syftet med be-

sök mellan parternas representanter är att säkerställa att överenskommelsens syfte om ett korrekt skydd för säkerhetsklassificerad information förverkligas. Denna besöksrätt innehåller inget sådant utövande av offentlig makt eller sådan granskningsrätt som står i konflikt med grundlagen (GrUU 39/1997 rd). I 18 § i lagen om internationella förpliktelser som gäller informationssäkerhet finns motsvarande föreskrifter om omständigheter i samband med genomförandet av överenskommelsens besöksbestämmelse. Artikeln hör till området för lagstiftningen, bortsett från punkt 2 som inte är skriven i förpliktande form.

I artikel 11 i överenskommelsen förutsätts att vardera parten utan dröjsmål underrättar den andra parten om upptäckta eller misstänkta kränkningar av dataskyddet som rör säkerhetsklassificerad information utbytt i enlighet med överenskommelsen. Parterna ska ytterligare, i enlighet med sina nationella lagar och bestämmelser, vidta alla relevanta åtgärder för att begränsa följderna av en kränkning av dataskyddet och undersöka incidenten. 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 interna-

tionella 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. Bestämmelserna 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 Schweiz om ömsesidigt skydd av säkerhetsklassificerad information kan inte anses innehålla bestämmelser som rör 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 Solothurn den 28 januari 2014 mellan Republiken Finlands regering och Schweiziska förbundsrådet 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 som hör till området för lagstiftningen i överenskommelsen med Schweiz om ömsesidigt skydd av säkerhetsklassificerad information

I enlighet med riksdagens beslut föreskrivs:

1 §

De bestämmelser som hör till området för lagstiftningen i den i Solothurn den 28 januari 2014 mellan Republiken Finlands regering och Schweiziska förbundsrådet 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 avtalet och om ikraftträdandet av denna lag bestäms genom förordning av statsrådet.

Helsingfors den 28 maj 2014

Statsminister

JYRKI KATAINEN

Utrikesminister *Erkki Tuomioja*

*Översättning**Fördragstext*

**ÖVERENSKOMMELSE
MELLAN REPUBLIKEN FINLANDS
REGERING OCH SCHWEIZISKA
FÖRBUNDSRÅDET OM ÖMSESIDIGT
SKYDD AV
SÄKERHETSKLASSIFICERAD
INFORMATION**

**AGREEMENT BETWEEN THE
GOVERNMENT OF THE REPUBLIC
OF FINLAND AND THE SWISS
FEDERAL COUNCIL ON MUTUAL
PROTECTION OF CLASSIFIED
INFORMATION**

Republiken Finlands regering och Schweiziska förbundsrådet, nedan kallade "parterna", som

beaktar att parterna kan men inte är förpliktade att utbyta säkerhetsklassificerad information i enlighet med denna överenskommelse,

är medvetna om att säkerhetsklassificerad information som utbyts ska hanteras i enlighet med principerna i denna överenskommelse,

för att skydda säkerhetsklassificerad information till exempel i frågor som rör utrikesärenden, försvar, säkerhet, vetenskap, företag eller teknik och som utbyts direkt mellan parterna eller mellan offentlig- eller privaträttsliga juridiska eller fysiska personer inom deras jurisdiktion som hanterar säkerhetsklassificerad information,

har kommit överens om följande:

Artikel 1

Syfte och tillämpningsområde

Syftet med denna överenskommelse är att säkerställa skyddet av sådan säkerhetsklassificerad information som utbyts eller framställs i samarbetet mellan parterna.

Artikel 2

Definitioner

I denna överenskommelse avses med

a) *säkerhetsklassificerad information* information, handlingar eller material, oavsett form, karaktär eller förmedlingssätt som en part lämnar ut till den andra parten och som har säkerhetsklassificerats och försetts med

The Government of the Republic of Finland and the Swiss Federal Council, hereinafter referred to as "the Parties",

bearing in mind that the Parties may but are not obliged to exchange Classified Information in the framework of this Agreement

recognising that when exchanging Classified Information it shall be handled in accordance with the principles governed in this Agreement

in order to protect Classified Information relating for example to foreign affairs, defence, security or scientific, industrial and technological matters and exchanged directly between the Parties, or public or private legal entities or individuals that deal with Classified Information under the jurisdiction of the Parties,

have agreed as follows:

Article 1

Purpose and scope of application

The purpose of this Agreement is to ensure the protection of Classified Information that is exchanged or created in the process of co-operation between the Parties.

Article 2

Definitions

For the purposes of this Agreement:

a) *Classified Information* means any information, document or material of whatever form, nature or method of transmission provided by one Party to the other Party and to which a security classification level has been

relevant anteckning om säkerhetsklass i enlighet med nationella lagar och bestämmelser, såväl som information, handlingar eller material som har framställts utifrån sådan säkerhetsklassificerad information och försetts med relevant anteckning om säkerhetsklass,

b) *säkerhetsklassificerat kontrakt* kontrakt eller underleverantörskontrakt, inbegripet förhandlingar som föregår kontrakt, som innehåller eller som har anknytning till säkerhetsklassificerad information,

c) *utlämnande part* den part och offentlig- eller privaträttsliga juridiska eller fysiska personer inom partens jurisdiktion som lämnar ut säkerhetsklassificerad information,

d) *mottagande part* den part och offentlig- eller privaträttsliga juridiska eller fysiska personer inom partens jurisdiktion till vilken den utlämnande parten lämnar ut säkerhetsklassificerad information,

e) *behörig säkerhetsmyndighet* nationell eller utsedd säkerhetsmyndighet eller annat behörigt organ som i enlighet med partens nationella lagar och bestämmelser har bemyndigats att ansvara för genomförandet av denna överenskommelse,

f) *kränkning av dataskyddet* en gärning eller försummelse som bryter mot nationella lagar och bestämmelser och som kan medföra att säkerhetsklassificerade uppgifter försvinner eller äventyras,

g) *säkerhetsutredning* ett positivt utfall av en prövning, baserad på nationella lagar och bestämmelser, av lämpligheten hos en juridisk person (säkerhetsutredning som gäller sammanslutning) eller en fysisk person (personsäkerhetsutredning) för tillgång till och hantering av säkerhetsklassificerade uppgifter på en bestämd nivå.

Artikel 3

Behöriga säkerhetsmyndigheter

1. Parterna har utsett följande nationella säkerhetsmyndigheter (National Security Authority, NSA) att ansvara för det allmänna genomförandet av denna överenskommelse:

applied and which has been marked accordingly under national laws and regulations, as well as any information, document or material that has been generated on the basis of such Classified Information and marked accordingly;

b) *Classified Contract* means any contract or sub-contract, including pre-contractual negotiations, which contains or involves Classified Information;

c) *Originating Party* means the Party, as well as any public or private legal entity or individual under its jurisdiction, releasing Classified Information;

d) *Receiving Party* means the Party, as well as any public or private legal entity or individual under its jurisdiction, to which the Classified Information is released by the Originating Party;

e) *Competent Security Authority* means a National Security Authority, a Designated Security Authority or any other competent body authorised according to the national laws and regulations of the Parties which is responsible for the implementation of this Agreement;

f) *Breach of Security* means an act or an omission contrary to national laws and regulations which may lead to the loss or compromise of Classified Information;

g) *Security Clearance* means a positive determination following an investigative procedure in accordance with national laws and regulations to ascertain the eligibility of an entity (Facility Security Clearance, FSC) or individual (Personnel Security Clearance, PSC) to have access to and to handle Classified Information on a certain level.

Article 3

Competent Security Authorities

1. The National Security Authorities (NSAs) designated by the Parties as responsible for the general implementation of this Agreement are:

I Republiken Finland	I Schweiziska edsförbundet
<i>Utrikesministeriet Nationella säkerhetsmyndigheten (NSA) FINLAND</i>	<i>Ministry of Defence Directorate for Information Security and Facility Protection (IOS) SWITZERLAND</i>

In the Republic of Finland	In the Swiss Confederation
<i>Ministry for Foreign Affairs National Security Authority (NSA) FINLAND</i>	<i>Ministry of Defence Directorate for Information Security and Facility Protection (IOS) SWITZERLAND</i>

2. Parterna ska underrätta varandra om eventuella andra behöriga säkerhetsmyndigheter som ansvarar för genomförandet av olika delar av denna överenskommelse.

3. Parterna ska underrätta varandra om eventuella senare ändringar i de behöriga säkerhetsmyndigheterna.

2. The Parties shall notify each other of any other Competent Security Authorities which shall be responsible for the implementation of aspects of this Agreement.

3. The Parties shall notify each other of any subsequent changes of the Competent Security Authorities.

Artikel 4

Article 4

Säkerhetsklasser

Security classifications

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

2. Säkerhetsklasserna motsvarar varandra enligt följande:

1. Any Classified Information provided under this Agreement shall be marked with the appropriate security classification level under the national laws and regulations of the Parties.

2. The classification levels shall correspond to one another as follows:

I Republiken Finland	I schweiziska edsförbundet	Motsvarighet på engelska
ERITTAIN SALAINEN eller YTTERST HEMLIG	ei vastinetta	TOP SECRET
SALAINEN eller HEMLIG	GEHEIM / SECRET / SEGRETO	SECRET
LUOTTAMUKSELLINEN eller KONFIDENTIELL	VERTRAULICH / CONFIDENTIEL/ CONFIDENZIALE	CONFIDENTIAL
KAYTTÖ RAJOITETTU eller BEGRÄNSAD TILLGÅNG	INTERN / INTERNE / AD USO INTERNO	RESTRICTED

In the Republic of Finland	In the Swiss Confederation	Equivalent in English
ERITTAIN SALAINEN or YTTERST HEMLIG	no equivalent	TOP SECRET
SALAINEN tai HEMLIG	GEHEIM / SECRET / SEGRETO	SECRET
LUOTTAMUKSELLINEN or KONFIDENTIELL	VERTRAULICH / CONFIDENTIEL/ CONFIDENZIALE	CONFIDENTIAL
KÄYTTÖ RAJOITETTU or BEGRÄNSAD TILLGÅNG	INTERN / INTERNE / AD USO INTERNO	RESTRICTED

3. I denna överenskommelse motsvarar de engelska uttrycken TOP SECRET, SECRET, CONFIDENTIAL och RESTRICTED de finländska och schweiziska termerna i tabellen ovan.

4. Den mottagande parten ska säkerställa att säkerhetsklasser inte ändras eller upphävs utan skriftligt tillstånd av den utlämnande parten.

5. Om Finland sänder information märkt YTTERST HEMLIIG, ska parternas behöriga säkerhetsmyndigheter sinsemellan komma överens om kompletterande arrangemang.

3. The English expressions TOP SECRET, SECRET, CONFIDENTIAL and RESTRICTED used in this Agreement correspond to the Swiss and Finnish terms in the table above.

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

5. In case Finland sends classified information marked TOP SECRET supplementary arrangements shall be agreed between the respective Competent Security Authorities.

Artikel 5

Skydd av säkerhetsklassificerad information

1. Parterna vidtar alla relevanta åtgärder i enlighet med sina nationella lagar och bestämmelser för att skydda säkerhetsklassificerad information som avses i denna överenskommelse. De ska skydda denna information på samma nivå som egen information i motsvarande säkerhetsklass.

2. Parterna ger inte tredje parter tillgång till säkerhetsklassificerad information utan den utlämnande partens skriftliga förhandssamtycke.

3. Tillgång till säkerhetsklassificerad information ska inskränkas till personer som

Article 5

Protection of Classified Information

1. The Parties shall take all appropriate measures under their national laws and regulations so as to protect Classified Information referred to in this Agreement. They shall afford such information the same protection as they afford to their own information at the corresponding classification level.

2. The Parties shall not provide access to Classified Information to Third Parties without the prior written consent of the Originating Party.

3. Access to Classified Information shall be limited to individuals who have a 'Need-to-

har ett informationsbehov, som har säkerhetsklarerats enligt nationella lagar och bestämmelser, som har bemyndigats att få tillgång till sådan information såväl som instruktioner om sitt ansvar i skyddet av säkerhetsklassificerad information.

4. Säkerhetsklassificerad information får endast användas för angivet ändamål.

Know' and who, in accordance with national laws and regulations, have been security cleared and authorised to have access to such information as well as briefed on their responsibilities for the protection of Classified Information.

4. Classified Information shall be used solely for the purpose for which it has been provided.

Artikel 6

Säkerhetsklassificerade kontrakt

1. Den mottagande partens behöriga säkerhetsmyndighet ska på begäran meddela den utlämnande partens behöriga säkerhetsmyndighet huruvida den föreslagna kontraktsparten hos den mottagande parten har beviljats nationellt intyg över säkerhetsutredning i den säkerhetsklass som krävs. Har kontraktsparten inte intyg över säkerhetsutredning, kan den utlämnande partens behöriga säkerhetsmyndighet be den mottagande partens behöriga säkerhetsmyndighet säkerhetsklara kontraktsparten.

2. Vid öppna anbudsförfaranden ska den mottagande partens behöriga säkerhetsmyndighet utan formell begäran överlämna de relevanta intygen över säkerhetsutredningar till den utlämnande partens behöriga säkerhetsmyndighet.

3. För tillräcklig övervakning och styrning av säkerheten ska säkerhetsklassificerade kontrakt som avses i bilaga 1 innefatta lämpliga säkerhetsbestämmelser, däribland klassificeringsanvisningar. En kopia av säkerhetsbestämmelserna ska skickas till den partens behöriga säkerhetsmyndigheter inom vars jurisdiktion det säkerhetsklassificerade kontraktet ska genomföras.

4. Representanter för parternas behöriga säkerhetsmyndigheter får på begäran besöka varandra för att bedöma effekten av de åtgärder som en kontraktspart har vidtagit för att skydda säkerhetsklassificerad information i anknytning till ett säkerhetsklassificerat kontrakt.

Article 6

Classified Contracts

1. Upon request, the Competent Security Authority of the Receiving Party shall inform the Competent Security Authority of the Originating Party whether a proposed contractor of the Receiving Party has been issued a national Facility Security Clearance corresponding to the required security classification level. If the contractor does not hold a Facility Security Clearance, the Competent Security Authority of the Originating Party may request that the contractor be security cleared by the Competent Security Authority of the Receiving Party.

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

3. To allow adequate security supervision and control a Classified Contract, referred to in Annex 1 to this Agreement, shall contain appropriate security provisions, including a classification guide. A copy of the security provisions shall be forwarded to the Competent Security Authority of the Party under whose jurisdiction the contract is to be performed.

4. Representatives of the Competent Security Authorities of the Parties may visit each other upon request in order to analyse the efficiency of the measures adopted by a contractor for the protection of Classified Information involved in a Classified Contract.

Artikel 7

Förmedling och registrering av säkerhetsklassificerad information

1. Parterna ska förmedla säkerhetsklassificerad information till varandra med hjälp av skyddade mellanstatliga kanaler eller så som de behöriga säkerhetsmyndigheterna annars kommer överens om.

2. Information i säkerhetsklass KONFIDENTIELL eller högre som utbyts mellan parterna ska registreras på ett lämpligt sätt och i enlighet med nationella lagar och bestämmelser.

Article 7

Transmission and registration of Classified Information

1. Classified Information shall be transmitted between the Parties through government-to-government secured channels or as otherwise agreed between their Competent Security Authorities.

2. Classified Information marked CONFIDENTIAL or higher exchanged between the Parties shall be duly registered according to national laws and regulations.

Artikel 8

Översättning, kopiering och utplåning av säkerhetsklassificerad information

1. Alla kopior och översättningar av säkerhetsklassificerad information ska förses med tillämplig anteckning om säkerhetsklass och skyddas på samma sätt som den säkerhetsklassificerade originalinformationen. Översättningarna och antalet kopior ska begränsas till det minimum det officiella syftet kräver.

2. Alla översättningar ska förses med en relevant anteckning på det översatta språket om att översättningen innehåller säkerhetsklassificerad information från den utlämnande parten.

3. Information i säkerhetsklass HEMLIG eller högre får översättas eller kopieras endast med skriftligt samtycke av den utlämnande parten.

4. Information i säkerhetsklass HEMLIG eller högre får inte utplånas utan den utlämnande partens skriftliga förhandssamtycke. Informationen ska returneras till den utlämnande parten när parterna anser att den inte längre behövs.

5. Information i säkerhetsklass KONFIDENTIELL ska utplånas när det anses att den inte längre behövs.

6. Om en krissituation förhindrar skyddet av säkerhetsklassificerad information som har lämnats ut i enlighet med denna överenskommelse, ska informationen omedelbart utplånas. Den mottagande parten ska så fort som möjligt underrätta den utlämnande par-

Article 8

Translation, reproduction and destruction of Classified Information

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

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

3. Classified Information marked SECRET or higher shall be translated or reproduced only upon the written consent of the Originating Party.

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

5. Classified Information marked CONFIDENTIAL shall be destroyed after it is no longer considered necessary.

6. If a crisis situation makes it impossible to protect Classified Information provided under this Agreement, the Classified Information shall be destroyed immediately. The Receiving Party shall notify the Competent Security Authority of the Originating Party

tens behöriga säkerhetsmyndighet om att den säkerhetsklassificerade informationen har utplånats.

about the destruction of the Classified Information as soon as possible.

Artikel 9

Article 9

Besök

Visits

1. Besök som omfattar tillgång till säkerhetsklassificerad information kräver skriftligt förhandstillstånd av värdpartens behöriga säkerhetsmyndighet. Besökare får tillgång till säkerhetsklassificerad information endast, om

1. Visits entailing a possibility of access to Classified Information require prior written authorisation from the Competent Security Authority of the host Party. Visitors shall only be allowed access where they have been:

a) den behöriga säkerhetsmyndigheten hos den part som sänder ut besökarna har beviljat tillstånd till besöket eller besöken de har bett om,

a) authorised by the Competent Security Authority of the sending Party to conduct the required visit or visits,

b) de har fått ett relevant intyg över person-säkerhetsundersökning, och

b) granted an appropriate Personnel Security Clearance, and

c) de har fått tillstånd att ta emot säkerhetsklassificerad information i enlighet med värdpartens lagar och bestämmelser.

c) authorised to receive Classified Information in accordance with the national laws and regulations of the host Party.

2. Den relevanta behöriga säkerhetsmyndigheten hos den part som föreslår besöket ska underrätta värdpartens relevanta behöriga säkerhetsmyndighet om det planerade besöket i enlighet med bestämmelserna i denna artikel och säkerställa att värdpartens behöriga säkerhetsmyndighet får begäran minst 14 dagar före den planerade tidpunkten för besöket. I brådskande fall får de behöriga säkerhetsmyndigheterna komma överens om en kortare tidsfrist. Besöksbegäran ska innehålla de uppgifter som avses i bilaga 2 till denna överenskommelse.

2. The relevant Competent Security Authority of the requesting Party shall notify the relevant Competent Security Authority of the host Party of the planned visit in accordance with the provisions laid down in this Article, and shall make sure that the latter receives the request for visit at least 14 days before the visit takes place. In urgent cases the Competent Security Authorities may agree on a shorter period. The request for visit shall contain the information referred to in Annex 2 to this Agreement.

3. Tillstånd för upprepade besök är giltiga i högst tolv (12) månader.

3. The validity of authorisations for recurring visits shall not exceed twelve (12) months.

Artikel 10

Article 10

Säkerhetssamarbete

Security co-operation

1. För verkställigheten av denna överenskommelse ska de nationella säkerhetsmyndigheterna informera varandra om sina relevanta nationella lagar och bestämmelser som gäller skyddet av säkerhetsklassificerad information och om eventuella senare ändringar i dem.

In order to implement this Agreement the National Security Authorities shall notify each other of their relevant national laws and regulations regarding the protection of Classified Information as well as of any subsequent amendments thereto.

2. I syfte att säkerställa ett nära samarbete i genomförandet av överenskommelsen ska de behöriga säkerhetsmyndigheterna samråda

2. In order to ensure close co-operation in the implementation of this Agreement the Competent Security Authorities shall consult

sinsemellan. De ska på begäran informera varandra om sina nationella säkerhetsnormer, förfaranden och tillämpningar för skyddet av säkerhetsklassificerad information. För att uppnå detta mål får de behöriga säkerhetsmyndigheterna besöka varandra.

3. De behöriga säkerhetsmyndigheterna ska i enlighet med sina nationella lagar och bestämmelser på begäran bistå varandra med att utföra säkerhetsklareringar.

4. De nationella säkerhetsmyndigheterna ska utan dröjsmål underrätta varandra om ändringar i de relevanta säkerhetsutredningarna.

5. Denna överenskommelse tillämpas inte på utbyte av säkerhetsklassificerad information mellan parternas underrättelsetjänster eller brottsbekämpande myndigheter (till exempel polisen).

Artikel 11

Kränkning av dataskyddet

1. Bägge parter ska utan dröjsmål underrätta den andra parten om upptäckta eller misstänkta kränkningar av dataskyddet som rör säkerhetsklassificerad information.

2. Bägge parter ska utan dröjsmål undersöka incidenten inom ramen för internationell rätt och sin nationella jurisdiktion. Den andra parten ska vid behov samarbeta med den behöriga parten i undersökningen.

3. Bägge parter ska inom ramen för internationell rätt och sin nationella jurisdiktion vidta alla relevanta åtgärder som är förenliga med nationella lagar och bestämmelser för att begränsa konsekvenserna av kränkningar av dataskyddet som avses i punkt 1 och för att förebygga ytterligare incidenter. Den andra parten ska underrättas om resultaten av undersökningen och vidtagna åtgärder.

Artikel 12

Kostnader

Vardera parten står för de kostnader som förorsakas dem genom verkställandet av förpliktelserna i denna överenskommelse.

each other. On request, they shall provide each other with information about their national security standards, procedures and practices for the protection of Classified Information. To this aim the Competent Security Authorities may visit each other.

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

4. The National Security Authorities shall promptly inform each other about changes in relevant security clearance certificates.

5. This Agreement does not apply to the exchange of Classified Information between the intelligence services and the law enforcement agencies (e.g. the police) of the two Parties.

Article 11

Breach of Security

1. Each Party shall immediately notify the other Party of any suspected or discovered Breach of Security of Classified Information.

2. Each Party shall, within the limits of the international law and its domestic jurisdiction, investigate the incident without delay. The other Party shall, if required, cooperate in the investigation of the Party with jurisdiction.

3. Each Party shall, within the limits of the international law and its domestic jurisdiction undertake all possible appropriate measures under its national laws and regulations so as to limit the consequences of breaches referred to in Paragraph 1 of this Article and to prevent further breaches. The other Party shall be informed of the outcome of the investigation and of the measures undertaken.

Article 12

Costs

Each Party shall bear its own costs incurred in the course of implementing its obligations under this Agreement.

Artikel 13

Twistlösning

Alla tvister mellan parterna som uppkommer angående tolkning eller tillämpning av denna överenskommelse ska uteslutande avgöras i samråd mellan parterna

Article 13

Resolution of disputes

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

Artikel 14

Slutbestämmelser

1. Parterna ska underrätta varandra när de nationella förfaranden som krävs för ikraftträdandet av överenskommelsen har slutförts. Överenskommelsen träder i kraft den första dagen den andra månaden efter att den senare underrättelsen har tagits emot.

2. Denna överenskommelse gäller tills vidare. Den kan ändras på gemensam skriftlig överenskommelse mellan parterna. En part kan när som helst föreslå ändringar i överenskommelsen. Om någondera parten föreslår ändringar, ska parterna inleda förhandlingar om en ändring av överenskommelsen.

3. En part kan säga upp överenskommelsen genom skriftlig anmälan till den andra parten via diplomatiska kanaler, iakttagande en uppsägningstid på sex (6) månader. Om överenskommelsen sägs upp, ska säkerhetsklassificerad information som redan har förmedlats eller som uppkommer genom överenskommelsen behandlas i enlighet med överenskommelsens bestämmelser så länge det är nödvändigt för att skydda informationen.

Denna överenskommelse ersätter samarbetsprotokollet mellan Finlands försvarsministerium och schweiziska försvarsministeriet om utbyte av säkerhetsklassificerad information som undertecknades den 17 mars 1994 i Bern.

Till bekräftelse härav har undertecknade, därtill vederbörligen bemyndigade, undertecknat denna överenskommelse

i Solothurm den 28 januari 2014.

i två exemplar på engelska.

Article 14

Final provisions

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

2. This Agreement shall be in force until further notice. The Agreement may be amended by the mutual, written consent of the Parties. Either Party may propose amendments to this Agreement at any time. If one Party so proposes, the Parties shall begin consultations on amending the Agreement.

3. Either Party may terminate this Agreement by written notification delivered to the other Party through diplomatic channels, observing a period of notice of six (6) months. If the Agreement is terminated, any Classified Information already provided and any Classified Information arising under the Agreement shall be handled in accordance with the provisions of the Agreement for as long as necessary for the protection of the Classified Information.

The present Agreement replaces the Memorandum of Understanding between the Ministry of Defence of Finland and the Ministry of Defence of Switzerland concerning the Exchange of Classified Information, signed in Berne on 17th March 1994.

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

in Solothurm on the 28th day of January, 2014.

in two duplicates in the English language.

För Republiken Finlands regering

For the Government of
the Republic of Finland

Alpo Rusi
Republiken Finlands ambassadör i Schweiz

Alpo Rusi
Ambassador of the Republic of Finland to
Switzerland

För schweiziska förbundsrådet

For the Swiss Federal Council

Urs Freiburghaus
Direktör för informations- och lokalitetssä-
kerhetsavdelningen

Urs Freiburghaus
Head of Directorate for Information Security
and Facility Protection

Bilaga 1

Bilaga 1

Säkerhetsklassificerade kontrakt

Kontrakt som avses i artikel 6 i denna överenskommelse ska innefatta följande uppgifter:

1. förfarande för att bemyndiga användare att hantera säkerhetsklassificerad information,
2. lagar och bestämmelser som utgör grunden för hantering av säkerhetsklassificerad information,
3. säkerhetsklass som krävs,
4. begränsningar i hanteringen av säkerhetsklassificerad information,
5. detaljerade bestämmelser om hur säkerhetsklassificerad information ska förmedlas,
6. detaljerade bestämmelser om hur säkerhetsklassificerad information ska hanteras,
7. märkning av säkerhetsklassificerad information och dess praktiska verkan,
8. uppgifter om de personer, däribland underleverantörer, som har rätt att få säkerhetsklassificerad information och förutsättningarna för detta,
9. krav som gäller skyddstiden för säkerhetsklassificerad information,
10. förfarande för hur säkerhetsklassificerad information ska utplånas eller returneras.

Annex 1

Classified Contracts

Classified Contracts referred to in Article 6 of this Agreement shall contain the following information:

1. procedure entitling a user to handle Classified Information
2. laws and regulations forming the base for the use of Classified Information
3. classification level required
4. limitations on the use of Classified Information
5. modalities of transmission of Classified Information
6. modalities of handling Classified Information
7. marking of Classified Information and practical consequences thereof
8. specifications of the persons, including sub-contractors, entitled to receive Classified Information and the conditions therefore
9. requirements for the period of protecting Classified Information
10. procedure for destroying or returning Classified Information

*Bilaga 2**Bilaga 2**Begäran om besök*

En begäran om besök som avses i artikel 9 i denna överenskommelse ska innefatta följande uppgifter:

1. besökarens för- och efternamn, födelseort och födelsetid/ursprung och nationalitet; besökarens ställning med uppgift om arbetsgivaren som besökaren företräder; uppgifter om projektet som besökaren deltar i samt nummer på besökarens pass eller annan identitetshandling,

2. bekräftelse på en personsäkerhetsutredning av besökaren motsvarande besökets ändamål,

3. syftet med besöket eller besöken, inkluderande den högsta nivån av säkerhetsklassificerade uppgifter som berörs,

4. planerad tidpunkt och längd för det begärda besöket eller de begärda besöken; vid återkommande besök anges om möjligt hela den period besöken avser,

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

6. datum samt den behöriga sändande säkerhetsmyndighetens underteckning och stämpel.

*Annex 2**Request for visit*

Requests for visit referred to in Article 9 of this Agreement shall contain the following information:

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

2. confirmation of Personnel Security Clearance of the visitor in accordance with the purpose of the visit;

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

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

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

6. the date, signature and seal of the sending Competent Security Authority.