

Regeringens proposition till riksdagen om godkännande och sättande i kraft av överenskommelsen mellan Finland och Österrike om ömsesidigt skydd av säkerhetsklassificerad information

PROPOSITIONENS HUVUDSAKLIGA INNEHÅLL

I denna proposition föreslås det att riksdagen godkänner en överenskommelse mellan Finland och Österrike om ömsesidigt skydd av säkerhetsklassificerad information och att riksdagen antar en lag för att sätta i kraft de bestämmelser i överenskommelsen som hör till området för lagstiftningen.

Syftet med överenskommelsen är att säkerställa skyddet av sådan säkerhetsklassificerad information som utbyts eller framställs i samarbetet mellan parterna särskilt i frågor som rör utrikesärenden, försvar, säkerhet och polis samt vetenskap, företag och teknik. Det är fråga om känsligt informationsmaterial som den utlämnande avtalsstaten särskilt har klassificerat på en nivå som kräver hög informationssäkerhet. Överenskommelsen förpliktar inte till utbyte av säkerhetsklassificerad information.

Parterna ska underrätta varandra när de nationella åtgärder som krävs för ikraftträdandet av överenskommelsen har slutförts. Överenskommelsen träder i kraft den första dagen den andra månaden efter det 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 föreskrivs genom förordning av statsrådet.

INNEHÅLL

| | |
|---|----|
| PROPOSITIONENS HUVUDSAKLIGA INNEHÅLL..... | 1 |
| INNEHÅLL | 2 |
| ALLMÅN MOTIVERING | 3 |
| 1 INLEDNING..... | 3 |
| 2 NULÄGE | 4 |
| 2.1 Lagen om internationella förpliktelser som gäller informationssäkerhet..... | 4 |
| Lagens allmänna tillämpningsområde..... | 4 |
| Lagens förhållande till offentlighetslagstiftningen | 5 |
| Tillämpning av lagen på näringsidkare | 5 |
| Verkställande myndigheter | 6 |
| Sekretess och reglering av informationsanvändningen | 6 |
| Säkerhetsklassificering och säkerhetsåtgärder | 6 |
| 2.2 Säkerhetsutredningslagen..... | 7 |
| Lagens syfte och tillämpningsområde..... | 7 |
| Personalsäkerhet..... | 7 |
| Företagssäkerhet..... | 8 |
| 3 MÅLSÄTTNING OCH DE VIKTIGASTE FÖRSLAGEN..... | 8 |
| 4 PROPOSITIONENS KONSEKVENSER | 9 |
| 4.1 Konsekvenser för medborgarna | 9 |
| 4.2 Konsekvenser för näringslivet | 9 |
| 4.3 Ekonomiska konsekvenser | 10 |
| 4.4 Konsekvenser för förvaltningen | 10 |
| 5 BEREDNINGEN AV PROPOSITIONEN | 10 |
| DETALJMOTIVERING | 11 |
| 1 ÖVERENSKOMMELSENS INNEHÅLL OCH FÖRHÅLLANDE TILL LAGSTIFTNINGEN I FINLAND..... | 11 |
| 2 LAGFÖRSLAG | 17 |
| 3 IKRAFTTRÄDANDE | 17 |
| 4 BEHOVET AV RIKSDAGENS SAMTYCKE SAMT BEHANDLINGSORDNING .. | 18 |
| 4.1 Behovet av riksdagens samtycke | 18 |
| 4.2 Behandlingsordning | 19 |
| LAGFÖRSLAG | 21 |
| om överenskommelsen med Österrike om ömsesidigt skydd av säkerhetsklassificerad information..... | 21 |
| FÖRDRAGSTEXT | 22 |

ALLMÄN MOTIVERING

1 Inledning

Med informationssäkerhet avses alla förfaranden som skyddar informationsinnehållet gentemot utomstående (informationens konfidentialitet), informationens oföränderlighet (integritet) samt informationens användbarhet (tillgänglighet vid behov). För att trygga informationssäkerheten tillämpas olika metoder: kontroll av personalens tillförlitlighet och verksamhetsutrymmenas säkerhet, sekretessbestämmelser och begränsningar av rätten att använda informationen till enbart 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.

Handlingar med anknytning till internationellt samarbete inbegriper ibland sådana sekretessbelagda uppgifter som, om de olovligen röjs, kan medföra avsevärd och utbredd skada för centrala allmänna intressen. Därför måste man särskilt se till att sådant material hanteras på tillbörligt sätt. Det gäller Finlands trovärdighet som part i det internationella samarbetet och skyddet av material som Finland lämnar ut. Det internationella informationssäkerhetssamarbetet, som även Finland är delaktigt i, omfattar sedvanligt skydd av icke-offentligt informationsutbyte som ingår i den diplomatiska verksamheten, liksom även i samarbetet mellan försvarsförvaltningarna. Utöver information som utbyts mellan stater har internationella förpliktelser som gäller informationssäkerhet växande betydelse också för det ekonomiska, industriella och tekniska samarbetet, där kommersiella projekt 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. Upphandling av det här slaget har traditionellt gällt särskilt försvarsområdet, men nuförtiden i allt högre grad också andra sektorer, såsom informationsteknologi och kärnkraftssektorn. En överenskommelse om informationssäkerhet ger företagen en avtalsram för genomförande av projekt så att finländska företag kan delta i upphandling inom sådana områden.

Finland har ingått bilaterala överenskommelser om informationssäkerhet med följande avtalsparter:

- Europeiska rymdorganisationen (ESA) (FördrS 94 och 95/2004)
- Tyskland (FördrS 96 och 97/2004)
- Frankrike (FördrS 66 och 67/2005)
- 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)
- Organisationen för gemensamt försvarsmaterielsamarbete i Europa (OCCAR) (FördrS 109 och 110/2008)
- Bulgarien (FördrS 116 och 117/2008)
- Slovenien (FördrS 22 och 23/2009)
- Tjeckien (FördrS 53 och 54/2009)
- Spanien (FördrS 38 och 39/2010)
- Nordatlantiska förbundet (Nato) (FördrS 7 och 8/2013)
- Amerikas förenta stater (FördrS 41 och 42/2013)
- Storbritannien (FördrS 49 och 50/2013)
- Luxemburg (FördrS 59 och 60/2013)
- Schweiz (FördrS 88 och 89/2014)

– Kroatien (FördrS 38 och 39/2015)

– Israel, där tillämpningsområdet är snävare och överenskommelsen gäller säkerhetsklassificerad information som förmedlas mellan försvars- och säkerhetsförvaltningarna (FördrS 34 och 35/2012).

Någon multilateral konvention inom området för informationssäkerhet finns inte. Ett undantag utgör det generella säkerhetsskyddsavtalet om ömsesidigt skydd och utbyte av säkerhetskyddsklassificerade uppgifter mellan Danmark, Finland, Island, Norge och Sverige (FördrS 11 och 12/2013). Avtalet mellan medlemsstaterna i EU om skydd av säkerhetsskyddsklassificerade uppgifter (FördrS 76 och 77/2015) trädde i kraft den 1 december 2015. Ett syfte med avtalet mellan Europeiska unionens medlemsstater är att inrätta en ram för skydd av nationellt säkerhetsskyddsklassificerade uppgifter som utbyts i Europeiska unionens intresse när medlemsstaterna inte har ingått något bilateralt avtal om informationssäkerhet. Bestämmelserna i det avtalet är dock inte lika övergripande som motsvarande bestämmelser i allmänna bilaterala överenskommelser om informationssäkerhet. Följaktligen eliminerar det inte behovet av bilaterala överenskommelser om informationssäkerhet mellan EU:s medlemsstater.

Genom överenskommelser om informationssäkerhet skapas förutsättningar för utbyte av säkerhetsklassificerad information mellan parterna. En överenskommelse säkerställer att säkerhetsklassificerat material som Finland lämnar ut hålls hemligt i mottagarlandet och att det skyddas och hanteras som det ska. Tack vare en informationssäkerhetsöverenskommelse kan också den andra parten försäkra sig om att Finland på ett korrekt sätt skyddar och hanterar säkerhetsklassificerad information som den lämnar ut.

2 Nuläge

2.1 Lagen om internationella förpliktelser som gäller informationssäkerhet

Lagens allmänna tillämpningsområde

Lagen om internationella förpliktelser som gäller informationssäkerhet (588/2004) tillämpas på särskilt känsligt informationsmaterial. Med det avses 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. Bestämmanderätten avseende utlämnad information kvarstår hos den utlämnande staten även efter det att informationen har utlämnats. Lagen kan tillämpas endast om en internationell överenskommelse 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 sådana handlingar som har upprättats av en finsk myndighet eller av en näringsidkare som omfattas av lagens tillämpningsområde och av vilka det framgår information som ingår i särskilt känsligt informationsmaterial som har sänts till Finland eller information som kan fås ur sådant material. Lagen tillämpas inte endast på hemlighållande eller klassificering av handlingar och delar av handlingar som innehåller nationell information från Finland.

Lagen innehåller bestämmelser om utfärdande av intyg över säkerhetsutredning av person (Personnel Security Clearance Certificate, PSCC) och säkerhetsutredning av företag (Facility Security Clearance Certificate, FSCC). För utfärdandet av intyg och prövningen i anslutning till detta ska den myndighet som gjort säkerhetsutredningen av person eller företag trots sekre-

RP 197/2017 rd

tessbestämmelserna lämna den nationella säkerhetsmyndigheten information om alla sådana omständigheter som vid utredningen framkommit i fråga om den person eller det företag som utredningen gäller (11 § 1 mom. och 12 § 1 mom.).

Vid bedömningen av huruvida ett intyg ska utfärdas, hur länge det ska vara giltigt och huruvida det ska återkallas tillämpas säkerhetsutredningslagen (11 § 2 mom. och 12 § 2 mom. i lagen om internationella förpliktelser som gäller informationssäkerhet). Om den nationella säkerhetsmyndigheten vägrar att utfärda ett intyg över säkerhetsutredning av person eller företag, ska den meddela skälen för detta i ett skriftligt beslut som ges till den som ansökt om utredningen och den som utredningen gäller (11 § 3 mom. och 12 § 3 mom. i lagen om internationella förpliktelser som gäller informationssäkerhet). Bestämmelser om ändringssökande finns i lagens 20 a §.

Lagens förhållande till offentlighetslagstiftningen

Lagen om internationella förpliktelser som gäller informationssäkerhet innehåller bestämmelser som avviker från bestämmelserna om informationssäkerheten som gäller nationella handlingar. I lagen ingår emellertid en allmän hänvisning till offentlighetslagen (3 § 1 mom.). Till de delar finska myndigheters handlingar innehåller annan information om internationellt samarbete än sådan som omfattas av internationella förpliktelser om informationssäkerhet, ska offentlighetslagen (621/1999) och med stöd av den utfärdade bestämmelser tillämpas. Enligt 3 § 2 mom. i lagen om internationella förpliktelser som gäller informationssäkerhet ska en på offentlighetslagen eller på någon annan lag baserad begäran om att få uppgifter ur särskilt känsligt informationsmaterial handläggas och avgöras av den myndighet till vilken informationsmaterialet har sänts eller som ska behandla ärendet i dess helhet.

Bestämmelserna i lagen om internationella förpliktelser som gäller informationssäkerhet ska tillämpas så länge det är nödvändigt på grund av det allmänna intresse som säkerhetsklassificeringen baserar sig på, också då den överenskommelse eller den författning som tillämpningen av bestämmelserna baserar sig på inte längre är i kraft (15 §). I fråga om när sekretessen upphör gäller vad som föreskrivs i offentlighetslagen. Enligt 31 § 2 mom. i offentlighetslagen är sekretesstiden för en myndighetshandling 25 år, om inte något annat föreskrivs. Enligt 31 § 3 mom. kan en handling vara sekretessbelagd även efter dessa 25 år, om den innehåller uppgifter som är säkerhetsklassificerade enligt lagen om internationella förpliktelser som gäller informationssäkerhet och om lämnande av uppgifter ur handlingen fortfarande skulle orsaka en sådan följd som avses i 24 § 1 mom. 2, 7 och 8 eller 10 punkten. Dessa handlingar blir enligt 31 § 3 mom. i offentlighetslagen offentliga när säkerhetsklassificeringen har upphävts.

Tillämpning av lagen på näringsidkare

Lagen om internationella förpliktelser som gäller informationssäkerhet tillämpas utöver 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 anbudsförfarande eller fullgörande av ett avtal kan förutsätta tillgång till särskilt känsligt informationsmaterial (2 § 1 mom. 3 punkten).

RP 197/2017 rd

En näringsidkare och den som är anställd av eller handlar på uppdrag av en näringsidkare har sekretessplikt i fråga om särskilt känsligt informationsmaterial, skyldighet att använda sådant material endast för angivet ändamål samt skyldighet att se till att endast personer som behöver informationen för skötsel av sina uppgifter har tillgång till materialet (6 §). För att uppfylla internationella förpliktelser som gäller informationssäkerhet är en näringsidkare också skyldig att lämna behöriga säkerhetsmyndigheter information samt att tillåta att representanter för myndigheter, internationella organ och fördragslutande stater bekantar sig med näringsidkarens säkerhetsarrangemang och verksamhetsutrymmen (16 § 2 mom. och 18 § 2 mom.).

Verkställande myndigheter

I 4 § i lagen om internationella förpliktelser som gäller informationssäkerhet finns bestämmelser om de myndigheter som ska se till att internationella förpliktelser som gäller informationssäkerhet uppfylls. Utrikesministeriet är Finlands nationella säkerhetsmyndighet (National Security Authority, NSA) i uppfyllandet av internationella förpliktelser som gäller informationssäkerhet. Försvarsministeriet, huvudstaben, Skyddspolisen och Kommunikationsverket är de utsedda säkerhetsmyndigheter (Designated Security Authority, DSA) som avses i internationella förpliktelser som gäller informationssäkerhet.

Sekretess och reglering av informationsanvändningen

Särskilt känsligt informationsmaterial ska sekretessbeläggas, om inte annat följer av en internationell förpliktelse som gäller informationssäkerhet (6 § 1 mom. i lagen om internationella förpliktelser som gäller informationssäkerhet). Sekretessplikten gäller också näringsidkare som är parter i säkerhetsklassificerade kontrakt. I Finlands bilaterala överenskommelser om utbyte och skydd av sekretessbelagd information mellan olika länders myndigheter ingår i regel en bestämmelse som begränsar användningen av den utlämnade informationen. Enligt bestämmelsen får särskilt känsligt informationsmaterial användas och överlätas 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 säkerhetsåtgärder

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

Enligt 10 § i lagen om internationella förpliktelser som gäller informationssäkerhet ska särskilt känsligt informationsmaterial förvaras i utrymmen där det är möjligt att skydda handlingarna och materialen samt informationen i dem i enlighet med en internationell förpliktelse som gäller informationssäkerhet. Bestämmelser om kraven på säkerheten i sådana utrymmen finns i 14 § i informationssäkerhetsförordningen.

Det allmänna kravet i internationella överenskommelser på att endast personer som behöver informationen för skötseln av sina uppgifter ska ges tillgång till den har skrivits in i lagen om internationella förpliktelser som gäller informationssäkerhet. Dessa personer ska i de fall som den internationella förpliktelsen som gäller informationssäkerhet förutsätter namnges på förhand (lagens 6 § 3 mom.). Detsamma gäller näringsidkare som avses 1 § 2 mom.

2.2 Säkerhetsutredningslagen

Lagens syfte och tillämpningsområde

Syftet med säkerhetsutredningslagen (726/2014) är att främja möjligheterna att förebygga verksamhet som kan medföra skada för statens säkerhet, försvaret, Finlands internationella förbindelser, den allmänna säkerheten eller något annat med dessa jämförbart allmänt intresse eller enskilda ekonomiska intressen av synnerligen stor betydelse eller säkerhetsarrangemang för skyddet av dessa intressen (1 §).

I lagen föreskrivs det om förfarandet vid genomförande av säkerhetsutredningar av personer och av företag. Lagen innehåller bestämmelser om förutsättningarna för säkerhetsutredningar och om vilka uppgifter som ska användas för utredningarna, om samtycke av och rätt till information för den som utredningen gäller, om uppgiftsskyldigheten för den som ansöker om säkerhetsutredning och den som utredningen gäller, om giltigheten av säkerhetsutredningar och intyg över säkerhetsutredningar och om återkallelse av intyg samt om samkörning av personregister för att kontrollera att den som utredningen gäller är oförvitlig och tillförlitlig och om de åtgärder som ska genomföras med anledning av samkörningen (2 §).

På grund av att integritetsskyddet har karaktär av grundläggande rättighet är säkerhetsutredningsförfarandet mycket formbundet. En säkerhetsutredning kan göras endast om den som utredningen gäller på förhand har gett sitt skriftliga samtycke (5 §).

Personalsäkerhet

Med säkerhetsutredning av person avses enligt 3 § 1 mom. 1 punkten i säkerhetsutredningslagen en sådan utredning av en fysisk persons bakgrund som görs i enlighet med den lagen för att säkerställa att han eller hon är oförvitlig eller tillförlitlig. Enligt lagens 23 § görs en säkerhetsutredning av person genom att registeruppgifter om personen kontrolleras på det sätt som föreskrivs i 4 kap. i lagen samt vid behov genom att personen intervjuas om sin situation i allmänhet, vistelse utomlands, utländska bindningar och relationer till medborgare i andra länder samt om andra sådana omständigheter som är av särskild betydelse för bedömningen av personens oberoende och tillförlitlighet i andra avseenden med tanke på de arbetsuppgifter som föranleder utredningen.

Enligt 14 § kan en säkerhetsutredning av person göras som en begränsad, en normal eller en omfattande säkerhetsutredning. Säkerhetsutredningar görs i de fall som anges i lagen, t.ex. om ett fördrag eller någon annan internationell förpliktelse som är bindande för Finland förutsätter att en säkerhetsutredning görs eller att ett intyg över en utredning visas upp.

Var och en har rätt att få information om huruvida det har gjorts en säkerhetsutredning om honom eller henne för något visst uppdrag. Den som utredningen gäller har även rätt att av den behöriga myndigheten på begäran få de uppgifter som finns i utredningen. Denna rätt gäller emellertid inte information som har sitt ursprung i personregister som en registrerad enligt lag inte har rätt till insyn i (6 §).

RP 197/2017 rd

I lagen finns en uttömmande förteckning över de register som får användas vid utredningsförfarandet. Säkerhetsutredningar får också bygga på vissa uppgifter i register som förs av en myndighet i en annan stat (25 §).

Enligt 43 § 2 mom. i säkerhetsutredningslagen utfärdar den nationella säkerhetsmyndigheten i enlighet med lagen om internationella förpliktelser som gäller informationssäkerhet sådana intyg över säkerhetsutredning av person som behövs för att uppfylla internationella förpliktelser som gäller informationssäkerhet.

Företagssäkerhet

I 33 § i säkerhetsutredningslagen föreskrivs det om rätten att ansöka om säkerhetsutredning av företag och i 36 § om förutsättningarna för säkerhetsutredning av företag. I 37 § finns en förteckning över informationskällorna vid säkerhetsutredning av företag, och 38 § handlar om handläggning av säkerhetsutredningar av företag. Vid en säkerhetsutredning av företag ska det med hjälp av uppgifterna i ansökan och de informationskällor som avses i 37 § samt genom inspektion av företagets lokaler och informationssystem utredas hur företaget kan se till att information skyddas, att obehörigt tillträde till lokalerna förhindras och att personalen får utbildning (38 § 1 mom.). En säkerhetsutredning av företag får också genomföras partiellt, om det behövs för att uppfylla en internationell förpliktelse som gäller informationssäkerhet eller om det annars är befogat (38 § 3 mom.). Internationellt används tre former av säkerhetsutredningar av företag: 1) en s.k. begränsad säkerhetsutredning av företag, ”FSC without safeguards”, som inte inbegriper inspektion av företagets lokaler eller informationssystem, 2) en säkerhetsutredning av företag, ”FSC with safeguards”, som inbegriper inspektion av lokalerna och 3) en säkerhetsutredning av företag, ”FSC with safeguards including Communications and Information Systems”, som inbegriper inspektion av lokaler och informationssystem.

Utredningen görs enligt 9 § i säkerhetsutredningslagen av Skyddspolisen. Det är dock huvudstaben som gör säkerhetsutredningen av ett företag när det är fråga om ett företag som sköter eller kommer att sköta ett uppdrag på förordnande av försvarsmakten eller ett företag som hänför sig till upphandling inom försvarsmakten. Kommunikationsverket har hand om bedömningen av informationssäkerheten i företags informationssystem och datakommunikation.

Den behöriga myndigheten kan enligt 40 § i säkerhetsutredningslagen, när den gör en säkerhetsutredning av företag och upprättar ett intyg över utredningen, förutsätta en förbindelse av företaget enligt vilken näringsidkaren förbinder sig att sörja för att informationssäkerhetsnivån bevaras och anmäla förändringar som inverkar på informationssäkerhetsnivån samt att för övervakning av att informationssäkerhetsnivån bevaras ge myndigheten tillstånd att komma in i företagets lokaler och lämna uppgifter som behövs för kontrollen.

Enligt lagens 46 § 2 mom. utfärdar den nationella säkerhetsmyndigheten i enlighet med lagen om internationella förpliktelser som gäller informationssäkerhet sådana intyg över säkerhetsutredning av företag som behövs för att uppfylla internationella förpliktelser som gäller informationssäkerhet.

3 Målsättning och de viktigaste förslagen

Syftet med denna proposition är att inhämta riksdagens godkännande för överenskommelsen. Överenskommelsen syftar till att säkerställa att säkerhetsklassificerad information som Finland lämnar ut till Österrike skyddas och hanteras korrekt. Överenskommelsen syftar också till att främja Finlands möjligheter att ta emot säkerhetsklassificerad information från Österrike och så förbättra samarbetet mellan länderna inom informationssäkerhetsområdet. Ytterligare syftar överenskommelsen till att trygga finländska företags möjligheter att delta i sådana inter-

nationella projekt eller projekt mellan Finland och Österrike som kan kräva utbyte av säkerhetsklassificerad information. Propositionen innehåller också ett förslag till en s.k. blankettlag för att sätta i kraft de bestämmelser i överenskommelsen som hör till området för lagstiftningen.

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 Österrike 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 Österrike gäller handlingar som Österrike anser att ska vara sekretessbelagda och följaktligen har försett med hög säkerhetsklassificering. I artikel 5 i överenskommelsen föreskrivs det om skyddet av och sekretessen för säkerhetsklassificerad information. Enligt artikel 5.2 får parterna inte ge tredje parter tillgång till säkerhetsklassificerad information utan den utlämnande partens skriftliga förhandssamtycke. Detta utgör ett undantag till offentlighetslagens bestämmelser om sekretessbeläggning i allmänt intresse, eftersom sekretessen där i de flesta fall är beroende av vilka konsekvenser för det skyddade intresset som uppstår av att uppgifter lämnas ut. Även utan överenskommelse om informationssäkerhet skulle säkerhetsklassificerade handlingar som Österrike lämnar ut till Finland i regel sekretessbeläggas med hänvisning till att de gäller internationella förhållanden i enlighet med 24 § 1 mom. 2 punkten i offentlighetslagen, vilket innebär att överenskommelsen om informationssäkerhet inte i större utsträckning än offentlighetslagen begränsar allmänhetens tillgång till information.

Den största skillnaden när lagen om internationella förpliktelser som gäller informationssäkerhet tillämpas i stället för offentlighetslagen 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 som föranleder klassificeringen, ska myndigheten kontakta den part som har upprättat handlingen.

Överenskommelsen om informationssäkerhet mellan Finland och Österrike 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 säkerhetsutredningslagen tillämpas för att kontrollera anställdas tillförlitlighet, innebär inte ett godkännande av den föreslagna ikraftträdandelagen att skyddet av medborgarnas personliga integritet och personuppgifter inskränks jämfört med tidigare.

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 Österrike.

Analogt öppnar överenskommelsen möjligheter för österrikiska 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 av kommande projekt. Projekt som inbegriper säkerhetsklassificerad information finns speciellt inom försvarsindustrin, säkerhet, kärnkraft, informationsteknik och andra högteknologiska sektorer samt inom vetenskap och forskning. Utan överenskommelse om informationssäkerhet kan finländska företag ställas utanför österrikiska projekt. Överenskommelsen syftar just till att på förhand bygga upp mekanismer och förfaranden 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 mer 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. Avtalet ökar i någon mån de uppgifter som enligt 4 § i lagen om internationella förpliktelser som gäller informationssäkerhet ska skötas av den nationella säkerhetsmyndigheten och de utsedda säkerhetsmyndigheterna.

Enligt överenskommelsens artikel 10.4 om säkerhetssamarbete ska säkerhetsmyndigheterna på begäran i enlighet med sina nationella lagar och bestämmelser bistå varandra med att utföra säkerhetsklareringar.

5 Beredningen av propositionen

Propositionen har beretts vid utrikesministeriet. Representanter för utrikesministeriet, försvarsministeriet, Skyddspolisen och Kommunikationsverket har deltagit i beredningen av och förhandlingarna om överenskommelsen. Propositionen har sänts på remiss till arbets- och näringsministeriet, finansministeriet, försvarsministeriet, inrikesministeriet, justitieministeriet, kommunikationsministeriet, Skyddspolisen, huvudstaben och Kommunikationsverket. Remissyttranden har kommit in från justitieministeriet, försvarsministeriet, arbets- och näringsministeriet, inrikesministeriet, Skyddspolisen och Kommunikationsverket. I sina yttranden förordar remissinstanserna att överenskommelsen ska godkännas och sättas i kraft.

DETALJMOTIVERING

1 Överenskommelsens innehåll och förhållande till lagstiftningen i Finland

Artikel 1. Syfte och tillämpningsområde. Enligt artikeln är syftet med överenskommelsen att säkerställa skyddet av sådan säkerhetsklassificerad information som utbyts eller framställs i samarbetet mellan parterna. Överenskommelsen tillämpas inte på sådan information som utbyts mellan parterna som inte är säkerhetsklassificerad. I Finland görs det t.ex. i regel inte någon anteckning om säkerhetsklassificering i polisens undersöknings- och underrättelseinformation.

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

I led a definieras säkerhetsklassificerad information. Överenskommelsen gäller information, handlingar eller material, oavsett form, karaktär eller förmedlingsätt som en part lämnar ut till den andra parten och som har säkerhetsklassificerats och märkts med klassificeringsanteckning i enlighet med nationella lagar och bestämmelser. Med säkerhetsklassificerad information avses vidare information, handlingar eller material som har framställts utifrån sådan säkerhetsklassificerad information och märkts med tillämplig klassificeringsanteckning. Detta led är i samklang med definitionen av särskilt känsligt informationsmaterial i 2 § 2 punkten i lagen om internationella förpliktelser som gäller informationssäkerhet.

Enligt led b avses med säkerhetsklassificerat kontrakt ett kontrakt eller underleverantörskontrakt som innehåller eller som har anknytning till säkerhetsklassificerad information. Detta led är i samklang med 2 § 3 punkten i lagen om internationella förpliktelser som gäller informationssäkerhet.

Enligt led c avses med utlämnande part den part som lämnar ut säkerhetsklassificerad information eller under vilken säkerhetsklassificerad information framställs.

Enligt led d avses med mottagare den part samt juridiska eller fysiska personer inom partens jurisdiktion till vilken den utlämnande parten lämnar ut säkerhetsklassificerad information.

Enligt led e avses med behörig säkerhetsmyndighet en nationell säkerhetsmyndighet, en utsedd säkerhetsmyndighet eller ett annat behörigt organ enligt artikel 3 som i enlighet med parternas nationella lagar och bestämmelser har bemyndigats att svara för genomförandet av överenskommelsen.

Enligt led f avses med kränkning av dataskyddet en sådan gärning eller försummelse i strid med nationella lagar och bestämmelser som kan medföra att säkerhetsklassificerad information går förlorad eller äventyras.

Enligt led g avses med säkerhetsutredning ett positivt utfall av en prövning, baserad på nationella lagar och bestämmelser, av lämpligheten hos en juridisk person (säkerhetsutredning av företag) eller en fysisk person (säkerhetsutredning av person) att få tillgång till och att hantera säkerhetsklassificerad information på en bestämd nivå.

Enligt led h avses med tredje part en stat som inte är part i överenskommelsen eller en juridisk eller fysisk person som inte omfattas av någondera partens jurisdiktion.

Artikel 3. Behöriga säkerhetsmyndigheter. I punkt 1 anges vardera partens nationella säkerhetsmyndigheter (National Security Authority, NSA) som ska svara för det allmänna genomförandet av överenskommelsen. Nationell säkerhetsmyndighet i Finland är enligt 4 § i lagen om internationella förpliktelser som gäller informationssäkerhet utrikesministeriet, där uppgiften sköts av Nationella säkerhetsmyndigheten (NSA). I Österrike har Information Security Commission (NSA)/Federal Chancellery utsetts till nationell säkerhetsmyndighet.

Enligt punkt 2 ska de nationella säkerhetsmyndigheterna underrätta varandra om eventuella andra behöriga säkerhetsmyndigheter (Competent Security Authorities, CSA) som till olika delar svarar för genomförandet av överenskommelsen och om senare ändringar i dessa myndigheter. Dessa underrättelser ska även innehålla kontaktuppgifter till de nationella säkerhetsmyndigheterna och till de andra behöriga säkerhetsmyndigheterna. Utsedda säkerhetsmyndigheter (Designated Security Authority, DSA) i Finland är enligt 4 § i lagen om internationella förpliktelser som gäller informationssäkerhet försvarsministeriet, huvudstaben, Skyddspolisens och Kommunikationsverket.

Artikel 4. Säkerhetsklasser. Enligt punkt 1 ska säkerhetsklassificerad information som lämnas ut i enlighet med överenskommelsen märkas med tillämplig anteckning om säkerhetsklass i enlighet med parternas nationella lagar och bestämmelser.

I punkt 2 definieras hur Finlands och Österrikes säkerhetsklasser motsvarar varandra. Den högsta säkerhetsklassen, som kräver de strängaste informationssäkerhetsåtgärderna, är ”ERITTÄIN SALAINEN/YTTERST HEMLIG” (”STRENG GEHEIM”). Till denna kategori räknas i Finland information som, om den obehörigen röjs, kan orsaka särskilt påtaglig skada för försvaret, säkerheten, de internationella relationerna eller andra allmänna intressen. Den näst högsta säkerhetsklassen är ”SALAINEN/HEMLIG” (”GEHEIM”). 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”), som i Finland avser information som, om den obehörigen röjs, kan skada försvaret, säkerheten, de internationella relationerna eller andra allmänna intressen. Till den fjärde säkerhetsklassen ”KÄYTTÖ RAJOITETTU/BEGRÄNSAD TILLGÅNG” (”EINGESCHRÄNKT”) hör information som, om den obehörigen röjs, kan skada allmänna intressen eller försämra myndigheternas möjligheter att agera.

Finlands internationella relationer skyddas i offentlighetslagens 24 § 1 mom. 1 och 2 punkt, försvaret i 10 punkten och säkerheten i 5, 8 och 9 punkten i samma moment. Andra allmänna intressen som avses i offentlighetslagen kan vara t.ex. 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 finns i 25 § i offentlighetslagen. Enligt 25 § 3 mom. i den lagen kan det i handlingen göras en anteckning som anger vilka krav på datasäkerhet som ska iakttas 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 så 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 eller med stöd av den förses med en sådan anteckning om säkerhetsklass som anges i en internationell förpliktelse som gäller informationssäkerhet och som anger vilka säkerhetskrav som ska iakttas vid hanteringen av materialet. Särskilda bestämmelser om anteckningen om säkerhetsklassificering finns i informationssäkerhetsförordningens 11 §, och

bestämmelser om anteckningarnas motsvarigheter i säkerhetsklasserna i internationella informationssäkerhetsförpliktelser finns i förordningens 12 §. I 11 § 1 mom. i förordningen finns bestämmelser om när en anteckning om säkerhetsklassificering kan göras i en sekretessbelagd handling. Enligt 11 § 3 mom. i förordningen 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 om handlingen inte i övrigt hänför sig till internationellt samarbete. En särskild bestämmelse om säkerhetsklassificeringsanteckningar på svenska finns i förordningens 11 § 4 mom.

Enligt punkt 3 i artikeln ska mottagaren säkerställa att säkerhetsklassificeringar inte ändras eller upphävs utan skriftligt tillstånd av den utlämnande parten. Den utlämnande parten ska utan dröjsmål meddela mottagaren, om säkerhetsklassen för utlämnad säkerhetsklassificerad information ändras eller upphävs.

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

Enligt punkt 1 ska parterna vidta alla relevanta åtgärder för att skydda säkerhetsklassificerad information som avses i överenskommelsen samt möjliggöra nödvändig övervakning av detta skydd. Parterna ska enligt samma punkt skydda denna information på samma sätt som de i enlighet med sina nationella lagar och bestämmelser skyddar egen information i motsvarande säkerhetsklass.

Enligt punkt 2 får parterna inte ge tredje parter tillgång till säkerhetsklassificerad information utan den utlämnande partens skriftliga förhandssamtycke. Denna punkt förpliktar parterna att följa principen om utlämnarens samtycke.

Enligt punkt 3 ska tillgång till säkerhetsklassificerad information inskränkas till personer som har ett informationsbehov och som i enlighet med nationella lagar och bestämmelser har säkerhetsklararats och bemyndigats att få tillgång till sådan information såväl som instruerats om sitt ansvar i skyddet av säkerhetsklassificerad information.

Enligt punkt 4 krävs inte säkerhetsutredning av person för tillgång till säkerhetsklassificerad information i säkerhetsklass KÄYTTÖ RAJOITETTU/BEGRÄNSAD TILLGÅNG eller ”EINGESCHRÄNK”.

Enligt punkt 5 får säkerhetsklassificerad information endast användas för angivet ändamål. En motsvarande bestämmelse finns i 6 § 2 mom. i lagen om internationella förpliktelser som gäller informationssäkerhet.

Enligt punkt 6 ska vardera parten inom tillämpningsområdet för överenskommelsen erkänna intyg över säkerhetsutredningar utfärdade av den andra parten.

Bestämmelserna i artikeln är i samklang med Finlands gällande lagstiftning om skydd av säkerhetsklassificerad information.

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

Enligt punkt 1 i artikeln ska mottagarens behöriga säkerhetsmyndighet på begäran meddela den utlämnande partens behöriga säkerhetsmyndighet huruvida det för den föreslagna kontraktsparten, som deltar i förhandlingar som föregår säkerhetsklassificerade kontrakt eller i

RP 197/2017 rd

genomförandet av ett sådant kontrakt, har utfärdats ett relevant intyg över säkerhetsutredning i den säkerhetsklass som krävs. Om kontraktsparten inte har ett sådant intyg över säkerhetsutredning, får den utlämnande partens behöriga säkerhetsmyndighet be mottagarens behöriga säkerhetsmyndighet säkerhetsklara kontraktsparten.

Enligt punkt 2 får vid öppna anbudsförfaranden mottagarens behöriga säkerhetsmyndighet utan formell begäran överlämna de relevanta intygen över säkerhetsutredningar till den utlämnande partens behöriga säkerhetsmyndighet.

Enligt punkt 3 krävs säkerhetsutredning av företag inte för tillgång till säkerhetsklassificerade kontrakt i säkerhetsklass KÄYTTÖ RAJOITETTU/BEGRÄNSAD TILLGÅNG eller ”INGESCHRÄNKT”.

Enligt punkt 4 ska säkerhetsklassificerade kontrakt, för att säkerheten ska kunna övervakas och kontrolleras i tillräcklig utsträckning, innefatta tillämpliga säkerhetsbestämmelser enligt bilaga 1 till överenskommelsen, däribland anvisningar om säkerhetsklassificering. Den utlämnande partens behöriga säkerhetsmyndighet ska skicka en kopia av säkerhetsbestämmelserna till mottagarens behöriga säkerhetsmyndighet.

Enligt punkt 5 ställs på underleverantörer samma säkerhetskrav, däribland i fråga om de relevanta intygen, som på den kontraktspart som har ingått ett säkerhetsklassificerat kontrakt.

Nationella bestämmelser om säkerhetsklassificerade kontrakt finns i 1 § 2 mom. (tillämpning på näringsidkare), 2 § 2 punkten (särskilt känsligt informationsmaterial), 2 § 3 punkten (säkerhetsklassificerat avtal), 6 § (sekretess och användning av information), 7 § (tystnadsplikt och förbud mot utnyttjande), 10 § (säkerhetskrav som gäller utrymmen), 12 § (intyg över säkerhetsutredning av företag, dess giltighet och återkallelse), 14 § (anteckning av uppgifter om intyg i registret över säkerhetsutredningar), 16 § (informationsskyldighet) och 18 § 2 mom. (besök av representanter för internationella organ och för fördragsslutande stater) i lagen om internationella förpliktelser som gäller informationssäkerhet. I 18 § 2 mom. i lagen om internationella förpliktelser som gäller informationssäkerhet föreskrivs det om skyldigheten för företag att tillåta att representanter för myndigheter, internationella organ och fördragsslutande stater bekantar sig med deras säkerhetsarrangemang och verksamhetsutrymmen, när det är nödvändigt för att uppfylla en internationell förpliktelse som gäller informationssäkerhet. I 40 § i säkerhetsutredningslagen föreskrivs det att företaget ska ge den behöriga myndigheten en förbindelse om att företaget bevarar sin informationssäkerhetsnivå och ger myndigheten tillstånd att komma in i företagets lokaler för att övervaka att säkerhetsnivån bevaras. Avtalsförpliktelserna enligt artikeln motsvarar kraven i den nationella lagstiftningen.

Artikel 7. Förmedling av säkerhetsklassificerad information. Artikeln innehåller bestämmelser om hur parterna ska förmedla säkerhetsklassificerad information till varandra i elektronisk och icke-elektronisk form.

Enligt punkt 1 ska parterna förmedla säkerhetsklassificerad information till varandra genom skyddade mellanstatliga kanaler eller på något annat sätt som har avtalats mellan deras behöriga säkerhetsmyndigheter. Mottagande av information i säkerhetsklass LUOTTAMUKSELLINEN/KONFIDENTIELL eller ”VERTRAULICH” eller högre ska bekräftas skriftligen.

Enligt punkt 2 får säkerhetsklassificerad information förmedlas elektroniskt mellan parterna endast på ett sådant säkert sätt som har avtalats mellan de behöriga säkerhetsmyndigheterna.

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

Artikel 8. *Översättning, kopiering och utplåning av säkerhetsklassificerad information.* Enligt punkt 1 i artikeln ska alla kopior och översättningar av säkerhetsklassificerad information vara försedda med tillämplig klassificeringsmärkning och skyddas på samma sätt som originalinformationen. Enligt samma punkt ska översättningarna och antalet kopior begränsas till det minimum det officiella syftet kräver.

Enligt punkt 2 ska alla översättningar förses med en tillämplig anteckning på det översatta språket om att de innehåller säkerhetsklassificerad information från den utlämnande parten.

Enligt punkt 3 får säkerhetsklassificerad information märkt ERITTÄIN SALAINEN/YTTERST HEMLIG eller ”STRENG GEHEIM” översättas eller kopieras endast med skriftligt samtycke av den utlämnande parten.

Enligt punkt 4 får säkerhetsklassificerad information märkt ERITTÄIN SALAINEN/YTTERST HEMLIG eller ”STRENG GEHEIM” inte utplånas utan skriftligt samtycke av den utlämnande parten. Informationen ska enligt samma punkt returneras till den utlämnande parten när parterna anser att den inte längre behövs.

Enligt punkt 5 ska säkerhetsklassificerad information märkt SALAINEN/HEMLIG eller ”GEHEIM”, eller med en lägre säkerhetsklass enligt artikel 4, förstöras när mottagaren anser att den inte längre behövs, i enlighet med mottagarens nationella lagar och bestämmelser.

Enligt punkt 6 ska informationen omedelbart utplånas, om en krissituation gör det omöjligt att skydda säkerhetsklassificerad information som har lämnats ut i enlighet med överenskommelsen. Den mottagande parten ska så fort som möjligt underrätta den utlämnande partens behöriga säkerhetsmyndighet om att den säkerhetsklassificerade informationen har utplånats i enlighet med punkt 6.

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 hanteras i något annat avseende finns i 9 § 1 mom. i lagen om internationella förpliktelser som gäller informationsssäkerhet. Närmare bestämmelser om hanteringen har i Finland utfärdats på förordningsnivå. I 17 § i informationssäkerhetsförordningen, som har utfärdats med stöd av offentlighetslagen, föreskrivs det om kopiering av handlingar och i 21 § om arkivering och förstöring av handlingar.

Artikel 9. *Besök.* Enligt punkt 1 krävs det för besök som inbegriper tillgång till säkerhetsklassificerad information i säkerhetsklass LUOTTAMUKSELLINEN/KONFIDENTIELL eller ”VERTRAULICH” eller högre skriftligt förhandstillstånd av värdpartens behöriga säkerhetsmyndighet. Enligt led a–b i samma punkt ska besökare få tillgång till sådan information endast, om den sändande partens behöriga säkerhetsmyndighet har gett dem tillstånd till det begärda besöket eller de begärda besöken och om de har fått ett relevant intyg över säkerhetsutredning av person.

Enligt punkt 2 ska den tillämpliga behöriga säkerhetsmyndigheten hos den part som föreslår besöket underrätta värdpartens tillämpliga behöriga säkerhetsmyndighet om det planerade besöket i enlighet med bestämmelserna i artikeln och se till att värdpartens säkerhetsmyndighet får besöksbegäran minst 14 dagar före den planerade tidpunkten för besöket. I brådskande fall kan de behöriga säkerhetsmyndigheterna komma överens om en kortare tidsfrist. Besöksbegäran ska innehålla de uppgifter som anges i bilaga 2 till överenskommelsen.

Enligt punkt 3 är tillstånd för upprepade besök giltiga i högst tolv (12) månader.

Artikel 10. Säkerhetssamarbete. I artikeln föreskrivs det om säkerhetssamarbetet mellan de nationella och de behöriga säkerhetsmyndigheterna.

Enligt punkt 1 ska de nationella säkerhetsmyndigheterna för att genomföra överenskommelsen informera varandra om sina tillämpliga nationella lagar och bestämmelser som gäller skyddet av säkerhetsklassificerad information och om eventuella senare ändringar i dem.

Enligt punkt 2 ska de behöriga säkerhetsmyndigheterna samråda sinsemellan i syfte att säkerställa ett nära samarbete i genomförandet av överenskommelsen och informera varandra om sina nationella säkerhetsnormer, förfaranden och tillämpningar för skyddet av säkerhetsklassificerad information och om väsentliga ändringar i dem. För detta ändamål kan de behöriga säkerhetsmyndigheterna avlägga besök hos varandra. Bestämmelser om besök finns i 18 § i lagen om internationella förpliktelser som gäller informationssäkerhet.

Enligt punkt 3 i artikeln kan de behöriga säkerhetsmyndigheterna även avlägga besök hos varandra för att diskutera genomförandet av en kontraktsparts åtgärder för att skydda säkerhetsklassificerad information i anknytning till ett säkerhetsklassificerat kontrakt.

Enligt punkt 4 ska säkerhetsmyndigheterna på begäran i enlighet med sina nationella lagar och bestämmelser bistå varandra med att utföra säkerhetsklareringar. Enligt 26 § 2 mom. 1 punkten i säkerhetsutredningslagen kan den behöriga myndighet som gör en säkerhetsutredning på tjänstens vägnar i enlighet med internationella avtal eller rättsregler från en utländsk myndighet inhämta en utredning som motsvarar de uppgifter som avses i 25 § 1 mom. 1–3 punkten och under vissa förutsättningar 4 punkten i säkerhetsutredningslagen. Avtalsförpliktelsen enligt denna punkt i artikeln motsvarar kraven i den nationella lagstiftningen.

Enligt punkt 5 ska de nationella säkerhetsmyndigheterna utan dröjsmål underrätta varandra om ändringar i relevanta intyg över säkerhetsutredningar.

Artikel 11. Kränkning av dataskyddet. Enligt punkt 1 ska vardera parten omedelbart skriftligen underrätta den andra parten om misstänkta eller upptäckta kränkningar av dataskyddet som rör säkerhetsklassificerad information som omfattas av överenskommelsen.

Enligt punkt 2 ska den part som har jurisdiktion utan dröjsmål undersöka misstänkta eller upptäckta kränkningar av dataskyddet. Den andra parten ska vid behov samarbeta i undersökningen.

Enligt punkt 3 ska den part som har jurisdiktion, i enlighet med sina nationella lagar och bestämmelser, vidta alla tillämpliga åtgärder som är möjliga för att begränsa konsekvenserna av de kränkningar av dataskyddet som avses i punkt 1 och för att förebygga ytterligare kränkningar. Den andra parten ska informeras om resultatet av utredningen och de genomförda åtgärderna.

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

Artikel 12. Kostnader. Enligt artikeln ska vardera parten bära sina egna kostnader för fullföljandet av förpliktelserna i överenskommelsen.

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

Artikel 14. Slutbestämmelser. Artikeln innehåller bestämmelser om ikraftträdande, ändring och uppsägning av överenskommelsen och om förpliktelser till följd av uppsägning.

Enligt punkt 1 i artikeln ska parterna underrätta varandra när de nationella åtgärder som krävs för ikraftträdandet av överenskommelsen har slutförts. Överenskommelsen träder i kraft den första dagen den andra månaden efter det att den senare underrättelsen har tagits emot.

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

Enligt punkt 3 kan en part 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 tillhandahållits eller som uppkommer genom överenskommelsen hanteras i enlighet med överenskommelsens bestämmelser så länge det är nödvändigt för att skydda informationen.

2 Lagförslag

I 95 § i grundlagen förutsätts det 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 inte är nödvändigt att justera det materiella innehållet i den nationella lagstiftningen till följd av förpliktelsen. Eftersom det inte är nödvändigt att ändra den materiella lagstiftningen för att genomföra förpliktelserna i överenskommelsen om informationssäkerhet mellan Finland och Österrike, innehåller propositionen endast ett förslag till blankettlag.

1 §. Enligt 1 § i lagförslaget ska de bestämmelser i överenskommelsen som hör till området för lagstiftningen gälla som lag. För de bestämmelser som hör till området för lagstiftningen redogörs det nedan i avsnittet om behovet av riksdagens samtycke.

2 §. Bestämmelser om sättande i kraft av de bestämmelser i överenskommelsen som inte hör till området för lagstiftningen ska enligt förslaget utfärdas genom förordning av statsrådet.

3 §. Bestämmelser om ikraftträdandet av lagen ska enligt förslaget utfärdas 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 Österrike ska parterna underrätta varandra när de nationella åtgärder som krävs för ikraftträdandet av överenskommelsen har slutförts. Enligt samma punkt träder överenskommelsen i kraft den första dagen den andra månaden efter det 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 föreskrivs genom förordning av statsrådet.

Överenskommelsen innehåller inga bestämmelser som faller inom landskapet Ålands behörighet och kräver därför inte landskapets bifall i enlighet med 59 § i självstyrelselagen för Åland (1144/1991).

4 Behovet av riksdagens samtycke samt behandlingsordning

4.1 Behovet av riksdagens samtycke

Enligt 94 § 1 mom. i grundlagen krävs riksdagens godkännande för fördrag och andra internationella förpliktelser som innehåller sådana bestämmelser som hör till området för lagstiftningen. Enligt grundlagsutskottets tolkningspraxis ska en bestämmelse anses höra till området för lagstiftningen, om den gäller utövande eller inskränkning av en grundläggande fri- eller rättighet som är tryggad i grundlagen, om den i övrigt gäller grunderna för individens rättigheter och skyldigheter, om det enligt grundlagen ska föreskrivas i lag om den sak som avses eller om det finns gällande bestämmelser i lag om saken eller om det enligt rådande uppfattning i Finland ska föreskrivas i lag om saken. Enligt grundlagsutskottet hör en bestämmelse i en internationell förpliktelse på dessa grunder till området för lagstiftningen oberoende av om den står i strid med eller harmonierar med en bestämmelse som utfärdats genom lag i Finland (se t.ex. GrUU 11/2000 rd och GrUU 12/2000 rd).

På de grunder som nämns ovan kräver flera bestämmelser i den överenskommelse som ingår i propositionen riksdagens samtycke. I artikel 2 i överenskommelsen definieras bland annat vad som avses med säkerhetsklassificerad information, säkerhetsklassificerat kontrakt, säkerhetsutredning och kränkning av dataskyddet. Eftersom dessa definitioner direkt eller indirekt påverkar tolkningen och tillämpningen av överenskommelsens materiella bestämmelser som hör till området för lagstiftningen, kräver de riksdagens godkännande (GrUU 6/2001 rd).

I artikel 3 i överenskommelsen definieras den nationella säkerhetsmyndigheten (NSA), som är underställd utrikesministeriet, som Finlands nationella säkerhetsmyndighet. Bestämmelsen motsvarar 4 § 1 mom. i lagen om internationella förpliktelser som gäller informationssäkerhet. Bestämmelsen är alltså konstaterande, och den har därför inte ansetts kräva riksdagens samtycke.

Artikel 4 innehåller bestämmelser om anteckningar om säkerhetsklass och om säkerhetsklassernas motsvarigheter. De allmänt tillämpliga bestämmelserna om anteckning om sekretess och klassificering finns i 25 § i offentlighetslagen. Enligt paragrafen ska det göras en anteckning om sekretess 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. Vidare finns det i 8 § i lagen om internationella förpliktelser som gäller informationssäkerhet bestämmelser om anteckning om säkerhetsklass när det gäller särskilt känsligt informationsmaterial. Enligt paragrafen 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 och som anger vilka säkerhetskrav som ska iakttas vid hanteringen av materialet. Bestämmelsen hör till området för lagstiftningen.

I artikel 5 i överenskommelsen föreskrivs det om åtgärder som krävs för att skydda säkerhetsklassificerad information inom överenskommelsens tillämpningsområde och som begränsar utlämnande, förmedling och användning av samt tillgången till informationen. Bestämmelsen i artikel 5.2 är överenskommelsens kärna. Enligt bestämmelsen får parterna inte ge tredje parter tillgång till säkerhetsklassificerad information utan den utlämnande partens skriftliga förhandssamtycke, och utifrån bestämmelsen kan Finland 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 och upptagningar. Denna rätt kan endast av tvingande skäl begränsas genom lag. Enligt

6 § 1 mom. i lagen om internationella förpliktelser som gäller informationssäkerhet ska särskilt känsligt informationsmaterial trots offentlighetslagens bestämmelser sekretessbeläggas, om inte annat följer av en internationell förpliktelse som gäller informationssäkerhet. I artikel 5.3 begränsas det vilka personer som kan få tillgång till säkerhetsklassificerad information. I artikel 5.3 föreskrivs det dessutom om parternas skyldighet att låta göra en lämplig säkerhetsutredning av personer som bemyndigas tillgång till sådan säkerhetsklassificerad information som avses i punkten. Det som i 10 § 1 mom. i grundlagen föreskrivs om skydd för privatlivet och om plikten att utfärda bestämmelser om skydd för personuppgifter genom lag ska beaktas i upplägget för säkerhetsutredningar. Bestämmelser om personer som är föremål för säkerhetsutredningar och om utredningsförfarandet finns i Finland i säkerhetsutredningslagen. Denna bestämmelse hör följaktligen till området för lagstiftningen och kräver riksdagens samtycke för att träda i kraft. Enligt artikel 5.5 i överenskommelsen får säkerhetsklassificerad information endast användas för angivet ändamål. En motsvarande bestämmelse finns i 6 § 2 mom. i lagen om internationella förpliktelser som gäller informationssäkerhet. Följaktligen hör bestämmelserna i artikeln till området för lagstiftningen.

I artikel 6 i överenskommelsen föreskrivs det om säkerhetsklassificerade kontrakt och om säkerhetsutredning av företag som ingår sådana kontrakt. På underleverantörer ställs samma säkerhetskrav som på den kontraktspart som har ingått ett säkerhetsklassificerat kontrakt. Bestämmelser om säkerhetsutredning av företag som förutsätts i en internationell förpliktelse som gäller informationssäkerhet och om det intyg som utfärdas med stöd av utredningen, dess giltighet och återkallelse finns i 12 § i lagen om internationella förpliktelser som gäller informationssäkerhet. Motsvarande bestämmelser om säkerhetsutredning av företag finns i säkerhetsutredningslagen.

I artikel 11 i överenskommelsen förutsätts det att de nationella säkerhetsmyndigheterna omedelbart ska underrätta varandra om misstänkta eller upptäckta kränkningar av dataskyddet som rör säkerhetsklassificerad information. Enligt samma artikel ska den part som har jurisdiktion utan dröjsmål undersöka händelsen. Vidare enligt samma artikel ska den part som har jurisdiktion i enlighet med sina nationella lagar och bestämmelser vidta alla tillämpliga åtgärder som är möjliga för att begränsa konsekvenserna av de kränkningar av dataskyddet som avses i artikeln och för att förebygga ytterligare kränkningar. Den andra parten ska informeras om resultatet av utredningen och de genomförda åtgärderna. I 19 § i lagen om internationella förpliktelser som gäller informationssäkerhet föreskrivs det om den nationella säkerhetsmyndighetens skyldigheter i sådana situationer som avses i bestämmelserna i överenskommelsen. Följaktligen hör bestämmelserna i artikeln till området för lagstiftningen.

4.2 Behandlingsordning

Allmänna bestämmelser om sekretessbeläggning av säkerhetsklassificerat informationsmaterial 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. Enligt 6 § 3 mom. ska en myndighet som hanterar särskilt känsligt informationsmaterial se till att endast personer som behöver informationen för skötsel av sina uppgifter har tillgång till materialet. Dessa personer ska i de fall som den internationella förpliktelsen som gäller informationssäkerhet förutsätter namnges på förhand. Detsamma gäller näringsidkare som avses i lagens 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 informat-

RP 197/2017 rd

ionssäkerhet. Bestämmelserna i artikel 5 i den föreliggande överenskommelsen utvidgar inte sekretessen utöver vad som föreskrivs om sekretess i lagens 6 §. Bestämmelserna inverkar följaktligen inte på överenskommelsens behandlingsordning.

Överenskommelsen mellan Finland och Österrike 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 Wien den 24 november 2017 mellan Republiken Finlands regering och Österrikes förbundsregering ingångna överenskommelsen om ömsesidigt skydd av säkerhetsklassificerad information.

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

Lag

om överenskommelsen med Österrike om ömsesidigt skydd av säkerhetsklassificerad information

I enlighet med riksdagens beslut föreskrivs:

1 §

De bestämmelser som hör till området för lagstiftningen i den i Wien den 24 november 2017 mellan Republiken Finlands regering och Österrikes förbundsregering ingångna överenskommelsen om skydd av säkerhetsklassificerad information ska gälla som lag, sådana som Finland har förbundit sig till dem.

2 §

Bestämmelser om sättande i kraft av de bestämmelser i överenskommelsen som inte hör till området för lagstiftningen utfärdas genom förordning av statsrådet.

3 §

Bestämmelser om ikraftträdandet av denna lag utfärdas genom förordning av statsrådet.

Helsingfors den 25 januari 2018

Statsminister

JUHA SIPILÄ

Utrikesminister Timo Soini

Fördragstext

**ÖVERENSKOMMELSE
MELLAN
REPUBLIKEN FINLANDS REGERING
OCH
ÖSTERRIKES FÖRBUNDSREGERING
OM
ÖMSESIDIGT SKYDD
AV SÄKERHETSKLASSIFICERAD
INFORMATION**

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

Republiken Finlands regering och Österrikes förbundsregering, nedan kallade ”parterna”, som

The Government of the Republic of Finland and the Austrian Federal Government, hereinafter referred to as “the Parties”,

för att skydda säkerhetsklassificerad information som särskilt rör utrikesärenden, försvar, säkerhet och polis samt vetenskap, företag och teknik och som utbyts direkt mellan parterna eller mellan juridiska eller fysiska personer inom deras jurisdiktion som hanterar säkerhetsklassificerad information,

in order to protect Classified Information related especially to foreign affairs, defence, security, police or scientific, industrial and technological matters and exchanged directly between the Parties, or legal entities or individuals that handle Classified Information under the jurisdiction of the Parties,

har kommit överens om följande:

have agreed as follows:

Artikel 1

Article 1

Syfte och tillämpningsområde

Purpose and scope of application

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

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

Artikel 2

Article 2

Definitioner

Definitions

I denna överenskommelse avses med

For the purposes of this Agreement:

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 märkts med klassificeringsanteckning i enlighet med någondera partens nationella lagar och bestämmelser i syfte att säkerställa skyddet av informationen mot sådan kränkning av data-skyddet som definieras i led f i denna artikel,

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 applied and which has been marked in accordance with the national laws and regulations of either Party, in order to ensure protection against a Breach of Security as defined in paragraph f) of this Article, as well

såväl som information, handlingar eller material som har framställts utifrån sådan säkerhetsklassificerad information och märkts med tillämplig klassificeringsanteckning,

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

c) *utlämnande part* part som lämnar ut säkerhetsklassificerad information eller under vilken säkerhetsklassificerad information framställs,

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

e) *behörig säkerhetsmyndighet* en nationell säkerhetsmyndighet, en utsedd säkerhetsmyndighet eller ett annat behörigt organ enligt artikel 3 som i enlighet med parternas nationella lagar och bestämmelser har bebyndigats att svara för genomförandet av denna överenskommelse,

f) *kränkning av dataskyddet* en sådan gärning eller försummelse i strid med någondera partens nationella lagar och bestämmelser som kan medföra att säkerhetsklassificerad information går förlorad eller äventyras,

g) *säkerhetsutredning* ett positivt utfall baserat på en utredning av lämpligheten hos en juridisk person (säkerhetsutredning av företag) eller en fysisk person (säkerhetsutredning av person) att få tillgång till och att hantera säkerhetsklassificerad information på en bestämd nivå i enlighet med nationella lagar och bestämmelser,

h) *tredje part* en stat som inte är part i denna överenskommelse eller en juridisk eller fysisk person som inte omfattas av någondera partens jurisdiktion.

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, which contains or involves Classified Information;

c) *Originating Party* means the Party which provides Classified Information or under whose authority Classified Information is generated;

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

e) *Competent Security Authority* means a National Security Authority, a Designated Security Authority or any other competent body authorised in accordance with the national laws and regulations of the Parties, which is responsible for the implementation of this Agreement, as specified in Article 3;

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

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

h) *Third Party* means any State that is not a Party to this Agreement or any legal entity or individual that is not under the jurisdiction of either Party.

Artikel 3

Behöriga säkerhetsmyndigheter

1. Följande nationella säkerhetsmyndigheter (National Security Authority, NSA) ska svara för det allmänna genomförandet av denna överenskommelse:

Article 3

Competent Security Authorities

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

RP 197/2017 rd

| | |
|--|---|
| I Republiken Finland | I Republiken Österrike |
| Utrikesministeriet Nationella säkerhetsmyndigheten (NSA) FINLAND | Federal Chancellery Information Security Commission (NSA) AUSTRIA |

| | |
|--|---|
| In the Republic of Finland: | In the Republic of Austria |
| Ministry for Foreign Affairs National Security Authority (NSA) FINLAND | Federal Chancellery Information Security Commission (NSA) AUSTRIA |

2. Parterna ska via diplomatiska kanaler underrätta varandra om eventuella andra behöriga säkerhetsmyndigheter som svarar för genomförandet av denna överenskommelse och om eventuella senare ändringar i dessa myndigheter. Dessa underrättelser ska även innehålla kontaktuppgifter till de nationella säkerhetsmyndigheterna och till de andra behöriga säkerhetsmyndigheterna.

2. The Parties shall notify each other through diplomatic channels of other Competent Security Authorities which are responsible for the implementation of this Agreement, as well as any subsequent changes thereof. Such notifications shall also include contact information on the NSAs and the other Competent Security Authorities.

Artikel 4

Säkerhetsklasser

1. Säkerhetsklassificerad information som lämnas ut i enlighet med denna överenskommelse ska märkas med tillämplig anteckning om säkerhetsklass i enlighet med parternas nationella lagar och bestämmelser.
2. Följande säkerhetsklasser motsvarar varandra:

Article 4

Security classifications

1. Any Classified Information provided under this Agreement shall be marked with the appropriate security classification level in accordance with the national laws and regulations of the Parties.
2. The classification levels shall correspond to one another as follows:

RP 197/2017 rd

| Republiken Finland | Republiken Österrike | Motsvarighet på engelska |
|---|-----------------------------|---------------------------------|
| ERITTÄIN SALAINEN eller YTTERST HEMLIG | STRENG GEHEIM | TOP SECRET |
| SALAINEN eller HEMLIG | GEHEIM | SECRET |
| LUOTTAMUKSELLINEN eller KONFIDENTIELL | VERTRAULICH | CONFIDENTIAL |
| KÄYTTÖ RAJOITETTU eller BEGRÄNSAD TILLGÅNG | EINGESCHRÄNKT | RESTRICTED |

| The Republic of Finland | The Republic of Austria | English translation |
|--|--------------------------------|----------------------------|
| ERITTÄIN SALAINEN or YTTERST HEMLIG | STRENG GEHEIM | TOP SECRET |
| SALAINEN or HEMLIG | GEHEIM | SECRET |
| LUOTTAMUKSELLINEN or KONFIDENTIELL | VERTRAULICH | CONFIDENTIAL |
| KÄYTTÖ RAJOITETTU or BEGRÄNSAD TILLGÅNG | EINGESCHRÄNKT | RESTRICTED |

3. Mottagaren ska säkerställa att säkerhetsklassificeringar inte ändras eller upphävs utan skriftligt tillstånd av den utlämnande parten. Den utlämnande parten ska utan dröjsmål meddela mottagaren, om säkerhetsklassen för utlämnad säkerhetsklassificerad information ändras eller upphävs.

3. The Recipient shall ensure that classifications are not altered or revoked, except as authorised in writing by the Originating Party. The Originating Party shall inform the Recipient without delay about any alteration or revocation of the security classification level of the transmitted Classified Information.

Artikel 5

Skydd av säkerhetsklassificerad information

Article 5

Protection of Classified Information

1. Parterna ska vidta alla relevanta åtgärder för att skydda säkerhetsklassificerad information som avses i denna överenskommelse och ska möjliggöra nödvändig övervakning av detta skydd. De ska skydda denna information åtminstone på samma sätt som de i enlighet med sina nationella lagar och bestämmelser skyddar egen information i motsvarande säkerhetsklass.

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

3. Tillgång till säkerhetsklassificerad information ska inskränkas till personer som har ett informationsbehov och som i enlighet med nationella lagar och bestämmelser har säkerhetsklarats och bemyndigats att få tillgång till sådan information såväl som instruerats om sitt ansvar i skyddet av säkerhetsklassificerad information.

4. Säkerhetsutredning av person krävs inte för tillgång till säkerhetsklassificerad information i säkerhetsklass KÄYTTÖ RAJOITETTU/BEGRÄNSAD TILLGÅNG eller EINGESCHRÄNKT.

5. Säkerhetsklassificerad information får endast användas för angivet ändamål.

6. Vardera parten ska inom tillämpningsområdet för denna överenskommelse erkänna intyg över säkerhetsutredningar utfärdade av den andra parten.

Artikel 6

Säkerhetsklassificerade kontrakt

1. Mottagarens behöriga säkerhetsmyndighet ska på begäran meddela den utlämnande partens behöriga säkerhetsmyndighet huruvida det för den föreslagna kontraktsparten, som deltar i förhandlingar som föregår säkerhetsklassificerade kontrakt eller i genomförandet av ett sådant kontrakt, har utfärdats ett relevant intyg över säkerhetsutredning i den säkerhetsklass som krävs. Om kontraktsparten inte har ett sådant intyg över säkerhetsutredning, får den utlämnande partens behöriga säkerhetsmyndighet be mottagarens behöriga säkerhetsmyndighet säkerhetsklara kontraktsparten.

2. Vid öppna anbudsförfaranden får motta-

1. The Parties shall take all appropriate measures to protect Classified Information referred to in this Agreement and shall provide for the necessary control of this protection. They shall afford such information at least the same protection as they afford to their own information at the corresponding classification level in accordance with their national laws and regulations.

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-know and who, in accordance with the 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. A Personnel Security Clearance is not required for access to Classified Information at the KÄYTTÖ RAJOITETTU / BEGRÄNSAD TILLGÅNG or EINGESCHRÄNKT level.

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

6. Within the scope of this Agreement, each Party shall recognize the Security Clearances issued by the other Party.

Article 6

Classified Contracts

1. Upon request, the Competent Security Authority of the Recipient shall inform the Competent Security Authority of the Originating Party whether a proposed contractor participating in precontract negotiations or in the implementation of a Classified Contract has been issued an appropriate Security Clearance corresponding to the required security classification level. If the contractor does not hold such a 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 Recipient.

2. In the case of an open tender the Compe-

garens behöriga säkerhetsmyndighet utan formell begäran överlämna de relevanta intygen över säkerhetsutredningar till den utlämnande partens behöriga säkerhetsmyndighet.

3. Säkerhetsutredning av företag krävs inte för tillgång till säkerhetsklassificerade kontrakt i säkerhetsklass KÄYTTÖ RAJOITETTU/BEGRÄNSAD TILLGÅNG eller EINGESCHRÄNKT.

4. För att säkerheten ska kunna övervakas och kontrolleras i tillräcklig utsträckning ska säkerhetsklassificerade kontrakt innefatta tillämpliga säkerhetsbestämmelser enligt bilaga 1 till denna överenskommelse, däribland anvisningar om säkerhetsklassificering. Den utlämnande partens behöriga säkerhetsmyndighet ska skicka en kopia av säkerhetsbestämmelserna till mottagarens behöriga säkerhetsmyndighet.

5. På underleverantörer ställs samma säkerhetskrav, däribland i fråga om de relevanta intygen, som på den kontraktspart som har ingått ett säkerhetsklassificerat kontrakt.

Artikel 7

Förmedling av säkerhetsklassificerad information

1. Parterna ska förmedla säkerhetsklassificerad information till varandra genom skyddade mellanstatliga kanaler eller på något annat sätt som har avtalats mellan deras behöriga säkerhetsmyndigheter. Mottagande av information i säkerhetsklass LUOTTAMUKSELLINEN/KONFIDENTIELL eller VERTRAULICH eller högre ska bekräftas skriftligen.

2. Säkerhetsklassificerad information får förmedlas elektroniskt mellan parterna endast på ett sådant säkert sätt som har avtalats mellan de behöriga säkerhetsmyndigheterna.

Artikel 8

Översättning, kopiering och utplåning av säkerhetsklassificerad information

1. Alla kopior och översättningar av säkerhetsklassificerad information ska vara försedda med tillämplig klassificeringsmärkning och skyddas på samma sätt som originalin-

tent Security Authority of the Recipient may provide the Competent Security Authority of the Originating Party with the relevant Security Clearance certificates without a formal request.

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

4. To allow adequate security supervision and control, a Classified Contract shall contain appropriate security provisions as specified in Annex 1, including a security classification guide. A copy of the security provisions shall be forwarded by the Competent Security Authority of the Originating Party to the Competent Security Authority of the Recipient.

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

Article 7

Transmission of Classified Information

1. Classified Information shall be transmitted between the Parties through secured government-to-government channels or as otherwise agreed between their Competent Security Authorities. Receipt of Classified Information marked LUOTTAMUKSELLINEN/KONFIDENTIELL or VERTRAULICH and above shall be acknowledged in writing.

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

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.

formationen. Översättningarna och antalet kopior ska begränsas till det minimum det officiella syftet kräver.

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

3. Säkerhetsklassificerad information märkt ERITTÄIN SALAINEN/YTTERST HEM-LIG eller STRENG GEHEIM får översättas eller kopieras endast med skriftligt samtycke av den utlämnande parten.

4. Säkerhetsklassificerad information märkt ERITTÄIN SALAINEN/YTTERST HEM-LIG eller STRENG GEHEIM får inte utplånas utan skriftligt samtycke av den utlämnande parten. Informationen ska returneras till den utlämnande parten när parterna anser att den inte längre behövs.

5. Säkerhetsklassificerad information märkt SALAINEN/HEMLIG eller GEHEIM, eller med en lägre säkerhetsklass enligt artikel 4, ska förstöras när mottagaren anser att den inte längre behövs, i enlighet med mottagarens nationella lagar och bestämmelser.

6. Om en krissituation gör det omöjligt att skydda säkerhetsklassificerad information som har lämnats ut i enlighet med denna överenskommelse, ska informationen utplånas omedelbart. Mottagaren ska så fort som möjligt underrätta den utlämnande partens behöriga säkerhetsmyndighet om att den säkerhetsklassificerade informationen har utplånats.

Artikel 9

Besök

1. För besök som inbegriper tillgång till säkerhetsklassificerad information i säkerhetsklass LUOTTAMUKSELLINEN/KONFIDENTIELL eller VERTRAULICH eller högre krävs skriftligt förhandstillstånd av värdpartens behöriga säkerhetsmyndighet. Besökare ska få tillgång till säkerhetsklassificerad information endast, om

a) den sändande partens behöriga säkerhetsmyndighet har gett dem tillstånd att avlägga det begärda besöket eller de begärda besöken, och

b) det för dem har utfärdats ett relevant in-

The translations and the number of reproductions shall be limited to the minimum required for an official purpose.

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

3. Classified Information marked ERITTÄIN SALAINEN / YTTERST HEM-LIG or STRENG GEHEIM shall be translated or reproduced only upon the written consent of the Originating Party.

4. Classified Information marked ERITTÄIN SALAINEN / YTTERST HEM-LIG or STRENG GEHEIM 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 SALAINEN/HEMLIG or GEHEIM or with a lower classification level under Article 4, shall be destroyed after it is no longer considered necessary by the Recipient, in accordance with its national laws and regulations.

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

Article 9

Visits

1. Visits entailing access to Classified Information at LUOTTAMUKSELLINEN/KONFIDENTIELL or VERTRAULICH or above require prior written permission from the Competent Security Authority of the host Party. Visitors shall only be allowed access where they have been:

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

b) granted an appropriate Personnel Securi-

tyg över säkerhetsutredning av person.

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

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

Artikel 10

Säkerhetssamarbete

1. De nationella säkerhetsmyndigheterna ska för att genomföra denna överenskommelse informera varandra om sina tillämpliga nationella lagar och bestämmelser som gäller skyddet av säkerhetsklassificerad information och om eventuella senare ändringar i dem.

2. I syfte att säkerställa ett nära samarbete i genomförandet av överenskommelsen ska de behöriga säkerhetsmyndigheterna samråda sinsemellan. De ska informera varandra om sina nationella säkerhetsnormer, förfaranden och tillämpningar för skyddet av säkerhetsklassificerad information och om väsentliga ändringar i dem. För detta ändamål kan de behöriga säkerhetsmyndigheterna avlägga besök hos varandra.

3. De behöriga säkerhetsmyndigheterna kan även avlägga besök hos varandra för att diskutera genomförandet av en kontraktsparts åtgärder för att skydda säkerhetsklassificerad information i anknytning till ett säkerhetsklassificerat kontrakt.

4. På begäran ska de behöriga säkerhetsmyndigheterna i enlighet med sina nationella lagar och bestämmelser bistå varandra med att utföra säkerhetsklareringar.

5. De nationella säkerhetsmyndigheterna ska utan dröjsmål underrätta varandra om ändringar i de intyg över säkerhetsutredningar som omfattas av denna överenskommelse.

ty Clearance.

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 specified in Annex 2 to this Agreement.

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

Article 10

Security co-operation

1. 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. In order to ensure close co-operation in the implementation of this Agreement the Competent Security Authorities shall consult each other. They shall provide each other with information about their national security standards, procedures and practices for the protection of Classified Information and any substantial changes thereof. To this aim the Competent Security Authorities may visit each other.

3. The Competent Security Authorities may also visit each other in order to discuss the implementation of the measures adopted by a contractor for the protection of Classified Information involved in a Classified Contract.

4. On request, Competent Security Authorities shall, in accordance with the national laws and regulations, assist each other in carrying out Security Clearance procedures.

5. The National Security Authorities shall promptly inform each other about changes of Security Clearance certificates falling under this Agreement.

Artikel 11

Kränkning av dataskyddet

1. Vardera parten ska omedelbart skriftligen underrätta den andra parten om misstänkta eller upptäckta kränkningar av dataskyddet som rör säkerhetsklassificerad information som omfattas av denna överenskommelse.

2. Den part som har jurisdiktion ska utan dröjsmål undersöka misstänkta eller upptäckta kränkningar av dataskyddet. Den andra parten ska vid behov samarbeta i undersökningen.

3. Den part som har jurisdiktion ska i enlighet med sina nationella lagar och bestämmelser vidta alla tillämpliga åtgärder som är möjliga för att begränsa konsekvenserna av de kränkningar av dataskyddet som avses i punkt 1 och för att förebygga ytterligare kränkningar. Den andra parten ska informeras om resultatet av utredningen och de genomförda åtgärderna.

Article 11

Breach of Security

1. Each Party shall immediately notify the other Party in writing of any suspected or discovered Breach of Security of Classified Information falling under this Agreement.

2. The Party with jurisdiction shall investigate suspected or discovered Breach of Security without delay. The other Party shall, if required, co-operate in the investigation.

3. The Party with jurisdiction shall undertake all possible appropriate measures in accordance with 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.

Artikel 12

Kostnader

Vardera parten ska bära sina egna kostnader för fullföljandet av förpliktelserna i denna överenskommelse.

Article 12

Costs

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

Artikel 13

Tvistlösning

Alla tvister mellan parterna som gäller tolkning eller tillämpning av denna överenskommelse ska utslutande 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 åtgärder som krävs för ikraftträ-

Article 14

Final provisions

1. The Parties shall notify each other of the completion of the national measures neces-

dandet av denna överenskommelse har slutförts. Överenskommelsen träder i kraft den första dagen den andra månaden efter det att den senare underrättelsen har tagits emot.

2. Denna överenskommelse gäller tills vidare. Överenskommelsen kan ändras på gemensam skriftlig överenskommelse mellan parterna. En part kan när som helst föreslå ändringar i överenskommelsen. Om endera 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 tillhandahållits eller som uppkommer genom överenskommelsen hanteras i enlighet med överenskommelsens bestämmelser så länge det är nödvändigt för att skydda informationen.

Till bekräftelse härav har representanter för parterna, därtill vederbörligen bemyndigade, undertecknat denna överenskommelse,

Wien den 24 november 2017

i två originalexemplar på finska, tyska och engelska, vilka alla texter är lika giltiga. I händelse av tolkningsskiljaktigheter ska den engelska texten gälla.

FÖR REPUBLIKEN FINLANDS
REGERING

Anu Laamanen

FÖR ÖSTERRIKES
FÖRBUNDSREGERING

Helmut Tichy

sary 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.

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

in Vienna on the 24th day of November, 2017

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

FOR THE GOVERNMENT OF THE
REPUBLIC OF FINLAND

Anu Laamanen

FOR THE AUSTRIAN
FEDERAL GOVERNMENT

Helmut Tichy

Bilaga 1

Säkerhetsklassificerade kontrakt

Säkerhetsklassificerade 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 regler om hur säkerhetsklassificerad information ska förmedlas,
6. detaljerade regler om hur säkerhetsklassificerad information ska hanteras,
7. märkning av säkerhetsklassificerad information och märkningens praktiska verkan,
8. uppgifter om de personer, däribland underleverantörer, som har rätt att ta emot säkerhetsklassificerad information och villkoren för mottagande,
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 therefor;
9. requirements for the period of protecting Classified Information;
10. procedure for destroying or returning Classified Information.

Bilaga 2

Besöksbegäran

En besöksbegäran som avses i artikel 9 i denna överenskommelse ska vara på engelska och innefatta följande uppgifter:

1. besökarens efternamn, förnamn, födelseort och -tid samt medborgarskap, besökarens ställning inklusive uppgift om vilken arbetsgivare besökaren företräder, uppgifter om det projekt besökaren deltar i samt numret på besökarens pass eller annat identitetsbevis,

2. bekräftelse på att besökaren har säkerhetsklararats i enlighet med besökets syfte,

3. syftet med besöket eller besöken, innefattande den högsta nivån av säkerhetsklassificerad information som berörs,

4. planerad tidpunkt och längd för begärt eller begärda besök; vid återkommande besök ska om möjligt hela den period besöken omfattar anges,

5. namn, adress, övriga kontaktuppgifter och kontaktperson till det organ eller den anläggning besöket avser samt annan information av vikt för att avgöra hur motiverat besöket eller besöken är,

6. datum samt den sändande behöriga säkerhetsmyndighetens underskrift och stämpel/sigill.

Annex 2

Request for visit

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

1. the visitor's family name, first name, place and date of birth and nationality, the visitor's position, with a specification of the employer which the visitor represents, a specification of the project in which the visitor participates, 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, other contact information and point of contact of the establishment or facility to be visited, and any other information useful for determining the justification for the visit or visits;

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