Regeringens proposition till riksdagen om godkännande och sättande i kraft av överenskommelsen med Ukraina om ömsesidigt skydd av säkerhetsklassificerad information

PROPOSITIONENS HUVUDSAKLIGA INNEHÅLL

I denna proposition föreslås det att riksdagen godkänner den i september 2019 undertecknade överenskommelsen mellan Finland och Ukraina om ömsesidigt skydd av säkerhetsklassificerad information och 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 och som särskilt rör utrikesärenden, försvar, säkerhet och brottsbekämpande samt vetenskapliga och tekniska frågor eller frågor som rör näringslivet. Det är fråga om sådant känsligt informationsmaterial som den utlämnande avtalsstaten särskilt har klassificerat på en nivå som kräver hög informationssäkerhet. Avtalet 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 i den andra månaden efter att den senare underrättelsen har tagits emot. Lagen om sättande i kraft av överenskommelsen avses träda i kraft samtidigt som överenskommelsen träder i kraft för Finlands del, vid en tidpunkt som föreskrivs genom förordning av statsrådet.

INNEHÅLL

MOTIVERING

1 Bakgrund och beredning

1.1 Bakgrund

Med informationssäkerhet avses alla förfaranden som skyddar informationsinnehåll gentemot utomstående (informationens konfidentialitet), informationens oföränderlighet (integritet) samt informationens användbarhet (tillgänglighet vid behov). För att trygga informationssäkerheten används olika metoder: säkerställande av personalens tillförlitlighet och lokalernas 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 som rör internationellt samarbete innehåller emellanåt sekretessbelagda uppgifter vars obehöriga röjande kan medföra betydande och omfattande skada för viktiga allmänna intressen. Det är därför nödvändigt att se till att sådant informationsmaterial behandlas korrekt. Det gäller Finlands trovärdighet som part i det internationella samarbetet och skyddet av material som Finland lämnar ut.

Det internationella informationssäkerhetssamarbetet, som även Finland deltar 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 emellertid också en växande betydelse för det ekonomiska, industriella och teknologiska samarbetet, där allt flera 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. Traditionellt hör upphandlingar av detta slag särskilt till försvarsområdet, men nuförtiden i allt högre grad också till anskaffningar inom andra sektorer, såsom informationsteknologi och kärnkraft. 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)
- Israel, där överenskommelsens tillämpningsområde är snävare och gäller säkerhetsklassificerad information som förmedlas mellan försvars- och säkerhetsförvaltningarna (FördrS 34 och 35/2012)
- Nordatlantiska förbundet (Nato) (FördrS 7 och 8/2013)
- Förenta staterna (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)
- Österrike (FördrS 37 och 38/2018)
- Ungern (FördrS 63 och 64/2018)

Det finns inte någon multilateral konvention inom området för informationssäkerhet. Ett undantag utgör det generella säkerhetsskyddsavtalet om ömsesidigt skydd och utbyte av säkerhetsskyddsklassificerade uppgifter mellan Danmark, Finland, Island, Norge och Sverige (FördrS 10, 11 och 12/2013). Ett avtal 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 detta avtal är dock inte lika täckande som motsvarande bestämmelser i allmänna bilaterala överenskommelser om informationssäkerhet. Följaktligen eliminerar det inte behovet av bilaterala överenskommelser om informationssäkerhet mellan EU:s medlemsstater.

Med överenskommelser om informationssäkerhet skapas förutsättningar för utbyte av säkerhetsklassificerad information mellan parterna. Genom en överenskommelse säkerställer man att säkerhetsklassificerad information som Finland lämnar ut hålls hemlig och hanteras korrekt i mottagarlandet. 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 parten lämnar ut.

1.2 Beredning

I februari 2016 föreslog Ukraina med en not från Ukrainas Finlandsambassad för Finland att länderna ingår en överenskommelse om informationssäkerhet. Finlands jakande svarsnot sändes till Ukraina i augusti 2016 och avtalsförhandlingar inleddes mellan Nationella säkerhetsmyndigheten och Ukrainas säkerhetstjänst.

De första diskussionerna om informationssäkerhetsöverenskommelsen med Ukraina fördes mellan förhandlingsdelegationerna den 1–2 november 2018 i Helsingfors. Därefter fortsatte förhandlingarna skriftligen under 2019. I beredningen och förhandlingarna deltog företrädare för utrikesministeriet, försvarsministeriet, skyddspolisen samt Transport- och kommunikationsverket. Överenskommelsen undertecknades den 12 september 2019 i Kiev.

Bestämmelser om ministeriernas ansvarsområden i fördragsärenden finns i 8 § i lagen om statsrådet (175/2003). Enligt paragrafens 1 mom. behandlas fördrag och andra internationella förpliktelser av det ministerium till vars ansvarsområde fördraget eller förpliktelsen enligt sakinnehållet hör. Propositionen har beretts vid utrikesministeriet.

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 sådant sekretessbelagt material samt information som kan fås fram ur dessa handlingar och detta material, och handlingar och material som framställts utifrån dem, som har säkerhetsklassificerats i enlighet med en internationell förpliktelse om informationssäkerhet. Bestämmanderätten över utlämnad information kvarstår även efter att den utlämnats hos

den utlämnande staten. Lagen kan endast tillämpas om den internationella överenskommelsen har satts i kraft i Finland på det sätt som grundlagen kräver eller om det är fråga om en internationell förpliktelse som annars är bindande för Finland.

Till kategorin särskilt känsligt informationsmaterial som omfattas av lagens tillämpningsområde hänförs ytterligare handlingar som har upprättats av en finsk myndighet eller av en näringsidkare som omfattas av lagens tillämpningsområde, av vilka framgår information som ingår i särskilt känsligt informationsmaterial som har sänts till Finland eller information som kan hämtas ur sådant material. Lagen tillämpas inte endast för 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, PSC) och säkerhetsutredning av företag (Facility Security Clearance, FSC). För utfärdandet av intyg och prövningen i anslutning till detta ska den myndighet som gjort säkerhetsutredningen av person eller företag trots sekretessbestämmelserna 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.).

I fråga om bedömning av huruvida ett intyg ska utfärdas samt om giltighet för och återkallelse av ett intyg 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

I lagen om internationella förpliktelser som gäller informationssäkerhet finns det bestämmelser som avviker från bestämmelserna om nationella handlingars informationssäkerhet. I lagens 3 § 1 mom. ingår emellertid en allmän hänvisning till offentlighetslagen (621/1999) och till informationshanteringslagen (906/2019). Till de delar finska myndigheters handlingar innehåller annan information om internationellt samarbete än sådan som omfattas av internationella förpliktelser om informationssäkerhet ska offentlighetslagen och bestämmelser som utfärdats med stöd av den 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 för 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 upphörande av sekretessförpliktelsen 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. Enligt 31 § 3 mom. i offentlighetslagen blir dessa handlingar offentliga när säkerhetsklassificeringen har upphävts.

Tillämpning av lagen på näringsidkare

Lagen om internationella förpliktelser som gäller informationssäkerhet tillämpas förutom på myndigheter också på en näringsidkare och dennes anställda i sådana fall då näringsidkaren är part i ett säkerhetsklassificerat avtal eller deltar i ett upphandlingsförfarande innan ett sådant avtal ingås eller är underleverantör för en sådan näringsidkare (1 § 2 mom.).

Med ett säkerhetsklassificerat avtal avses ett avtal som en myndighet i en annan stat eller ett företag som har hemvist i den andra staten eller en internationell organisation eller ett internationellt organ, på det sätt som avses i en internationell förpliktelse som gäller informationssäkerhet, har för avsikt att ingå eller har ingått med en näringsidkare som har hemvist i Finland, om deltagande i ett anbudsförfarande eller fullgörande av ett avtal kan förutsätta tillgång till särskilt känsligt informationsmaterial (2 § 1 mom. 3 punkten).

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 låta representanter för myndigheter, internationella organ och fördragsslutande stater bekanta sig med sina säkerhetsarrangemang och lokaler (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 ser till att de internationella förpliktelserna 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 Transport- och kommunikationsverket är utsedda säkerhetsmyndigheter (Designated Security Authority, DSA).

Sekretessbeläggning och reglering av informationsanvändningen

Särskilt känsligt informationsmaterial ska sekretessbeläggas, om inte annat följer av en internationell förpliktelse som gäller informationssäkerhet (lagen om internationella förpliktelser som gäller informationssäkerhet, 6 § 1 mom.). Sekretessplikten gäller också näringsidkare som är parter i säkerhetsklassificerade kontrakt. I Finlands bilaterala överenskommelser om utbyte av sekretessbelagd information mellan olika länders myndigheter ingår i regel en bestämmelse som begränsar användningen av den utlämnade informationen. Enligt den bestämmelsen får särskilt känsligt informationsmaterial användas och överlåtas endast för angivet ändamål, om inte den som har klassificerat materialet samtycker till något annat. Användningen av särskilt känsligt informationsmaterial är alltså strikt ändamålsbunden.

Säkerhetsklassificering och säkerhetsåtgärder

I lagen om internationella förpliktelser som gäller informationssäkerhet föreskrivs om skyldigheten att förse särskilt känsligt informationsmaterial med anteckning om säkerhetsklass. Anteckningen anger vilka åtgärder som ska vidtas vid hantering av materialet (8 §). Ju högre materialets säkerhetsklass är, desto strängare säkerhetsåtgärder krävs det. Lagen innehåller en allmän förpliktelse att tillämpa de bestämmelser om hantering av informationsmaterialet som materialets säkerhetsklass förutsätter samt ett bemyndigande att genom förordning av statsrådet föreskriva om säkerhetsåtgärder vid hantering av särskilt känsligt informationsmaterial som motsvarar de olika säkerhetsklasserna (9 §). I 4 § i statsrådets förordning om säkerhetsklassificering av handlingar

inom statsförvaltningen (1101/2019), nedan kallad *säkerhetsklassificeringsförordningen,* finns det 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 9 och 10 § i säkerhetsklassificeringsförordningen.

Det allmänna kravet i internationella överenskommelser om 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 namnges på förhand i de fall som den internationella förpliktelsen som gäller informationssäkerhet förutsätter (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 person och av företag. Lagen innehåller bestämmelser om förutsättningarna för säkerhetsutredningar och om vilka uppgifter som ska användas för en säkerhetsutredning, samtycke av och rätt till information för den som utredningen gäller, uppgiftsskyldigheten för den som ansöker om säkerhetsutredning och den som utredningen gäller, giltigheten av säkerhetsutredningar och intyg över säkerhetsutredningar samt 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 §).

Eftersom integritetsskyddets har karaktären av en grundläggande rättighet är säkerhetsutredningsförfarandet strikt formbundet. En säkerhetsutredning kan göras endast om den som utredningen gäller på förhand har gett sitt skriftliga samtycke till detta (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 23 § i lagen görs en säkerhetsutredning av person genom att registeruppgifter om den personen kontrolleras på det sätt som föreskrivs i kapitlet samt vid behov genom att personen intervjuas om sin situation i allmänhet, vistelse utomlands och sina relationer till medborgare i andra länder samt om andra omständigheter som är av särskild betydelse för bedömningen av hans eller hennes tillförlitlighet med tanke på de arbetsuppgifter som utredningen görs för.

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, till exempel om ett fördrag eller någon annan internationell förpliktelse som är bindande för Finland förutsätter att en säkerhetsutredning ska göras eller att ett intyg över en utredning visas upp.

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

I lagen finns också en uttömmande uppräkning över de register som får användas vid utredningsförfarandet. Informationskällorna för 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 bestäms om rätten att ansöka om säkerhetsutredning av företag och i 36 § om förutsättningar för säkerhetsutredning av företag. I 37 § förtecknas informationskällorna vid säkerhetsutredning av företag och 38 § handlar om handläggning av säkerhetsutredningar av företag. Vid en säkerhetsutredning av företag ska det med hjälp av uppgifterna i ansökan och de informationskällor som avses i 37 § samt genom inspektion av företagets lokaler och dess informationssystem utredas hur företaget kan se till att information skyddas, obehörigt tillträde till lokalerna förhindras och 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 för att syftet med säkerhetsutredningen ska uppnås (38 § 3 mom.). Internationellt används tre former av säkerhetsutredningar av företag: 1) begränsad säkerhetsutredning av företag som inte inbegriper inspektion av företagets lokaler eller informationssystem ”FSC without safeguards”, 2) säkerhetsutredning av företag som inbegriper inspektion av lokalerna ”FSC with safeguards” och 3) säkerhetsutredning av företag som inbegriper inspektion av lokaler och informationssystem ”FSC with safeguards including Communications and Information Systems”.

Denna utredning 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 om ett företag som hänför sig till upphandling inom försvarsmakten. Transport- och kommunikationsverket har hand om bedömningen av informationssäkerheten i informationssystem och datakommunikation.

Enligt 40 § i säkerhetsutredningslagen kan den behöriga myndigheten när den gör en säkerhetsutredning av företag och upprättar ett intyg över utredningen förutsätta att 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 Överenskommelsens syfte

Överenskommelsen syftar till att säkerställa att säkerhetsklassificerad information som Finland lämnar ut till Ukraina skyddas och hanteras korrekt. Överenskommelsen syftar också till att främja Finlands möjligheter att ta emot säkerhetsklassificerad information från Ukraina och så förbättra samarbetet mellan länderna inom in-

formationssäkerhetsområdet. Ytterligare syftar överenskommelsen till att trygga finländska företags möjligheter att delta i sådana internationella projekt eller projekt mellan Finland och Ukraina som kan kräva utbyte av säkerhetsklassificerad information.

4 De viktigaste förslagen

I denna proposition föreslås det att riksdagen godkänner överenskommelsen mellan Finland och Ukraina om ömsesidigt skydd av säkerhetsklassificerad information. Propositionen innehåller också ett förslag till så kallad blankettlag genom vilken de bestämmelser i avtalet som hör till området för lagstiftningen sätts i kraft.

5 Propositionens konsekvenser

5.1 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 Ukraina 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 Ukraina gäller handlingar som Ukraina anser att ska vara sekretessbelagda och följaktligen har försett med hög säkerhetsklassificering. I artikel 5 i överenskommelsen föreskrivs om skyddet av och om sekretessen med avseende på säkerhetsklassificerad information. Enligt artikel 5.2 ger parterna inte tredje parter tillgång till säkerhetsklassificerad information utan den utlämnande partens skriftliga förhandssamtycke. Detta utgör ett undantag till bestämmelserna i offentlighetslagen om sekretessbeläggning i allmänt intresse, eftersom sekretessen där i de flesta fall är beroende av konsekvenserna för det skyddade intresset av att uppgifter lämnas ut. Även utan överenskommelse om informationssäkerhet skulle säkerhetsklassificerade handlingar som Ukraina lämnar ut till Finland i regel sekretessbeläggas med stöd av 24 § 1 mom. 2 punkten i offentlighetslagen, vilket innebär att överenskommelsen om informationssäkerhet inte begränsar allmänhetens tillgång till information dess mera än offentlighetslagen.

Den största skillnaden 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 det är som föranleder klassificeringen, ska myndigheten kontakta den part som har upprättat handlingen.

Överenskommelsen om informationssäkerhet mellan Finland och Ukraina 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 används för att kontrollera anställdas tillförlitlighet, innebär ett godkännande av den föreslagna ikraftträdandelagen inte inskränkningar jämfört med tidigare i skyddet av medborgarnas personliga integritet och personuppgifter.

5.2 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 Ukraina. Analogt öppnar överenskommelsen möjligheter för ukrainska företag att få beställningar eller att delta i projekt som förutsätter tillgång till information som är säkerhetsklassificerad i Finland. Det är svårt att på förhand uppskatta antalet och det ekonomiska värdet på kommande projekt.

Projekt som 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 ukrainska projekt. Överenskommelsen syftar just till att bygga upp mekanismer och förfaranden på förhand för att det ska vara möjligt att delta i projekt och till att på detta sätt förbättra finländska företags konkurrenskraft.

5.3 Ekonomiska konsekvenser

Propositionen har inga konsekvenser för statsbudgeten eller några andra mer än obetydliga ekonomiska konsekvenser.

5.4 Konsekvenser för förvaltningen

Godkännandet av den överenskommelse och den lag som ingår i propositionen medför inga skyldigheter till eller behov av förändringar i förvaltningen. Överenskommelsen ökar i någon mån sådana uppgifter som den nationella säkerhetsmyndigheten och de utsedda säkerhetsmyndigheterna har ålagts enligt 4 § i lagen om internationella förpliktelser som gäller informationssäkerhet.

I enlighet med överenskommelsens artikel 10.3 om säkerhetssamarbete ska säkerhetsmyndigheterna på begäran bistå varandra i enlighet med nationella lagar och bestämmelser vid utarbetandet av säkerhetsutredningar av personer och företag.

6 Remissvar

Utlåtanden om propositionen har begärts av arbets- och näringsministeriet, finansministeriet, försvarsministeriet, inrikesministeriet, justitieministeriet, kommunikationsministeriet, skyddspolisen, Huvudstaben och Transport- och kommunikationsverket. Försvarsministeriet, kommunikationsministeriet, Huvudstaben, Transport- och kommunikationsverket samt skyddspolisen lämnade utlåtanden. I utlåtandena förordas att överenskommelsen godkänns och sätts i kraft.

7 Bestämmelserna i avtalet och deras förhållande till lagstiftningen i Finland

Artikel 1. *Syfte och tillämpningsområde.* I artikeln definieras att syftet med överenskommelsen är att säkerställa skyddet av säkerhetsklassificerad information som utbyts eller framställs i samarbetet mellan parterna. Överenskommelsen tillämpas inte på sådan information som utbyts mellan parterna som inte är säkerhetsklassificerad.

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

I punkt a definieras säkerhetsklassificerad information. Överenskommelsen gäller information, handlingar eller material, oavsett form, som har säkerhetsklassificerats och försetts med klassificeringsanteckning i enlighet med nationella lagar och bestämmelser. Med säkerhetsklassificerad information avses vidare information, handlingar eller material som har framställts utifrån från sådan säkerhetsklassificerad information och försetts

med tillämplig klassificeringsanteckning. Denna punkt är i samklang med definitionen av särskilt känsligt informationsmaterial i 2 § 1 mom. 2 punkten i lagen om internationella förpliktelser som gäller informationssäkerhet.

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

Enligt punkt c avses med utlämnande part den part som lämnar ut säkerhetsklassificerad information.

Enligt punkt d avses med mottagande part den part och offentligrättsliga eller privaträttsliga juridiska eller fysiska personer inom partens jurisdiktion till vilken den utlämnande parten lämnar ut säkerhetsklassificerad information.

Enligt punkt e avses med behörig säkerhetsmyndighet nationell säkerhetsmyndighet eller särskilt utsett statligt organ som i enlighet med parternas nationella lagar och bestämmelser har bemyndigats att svara för genomförandet av överenskommelsen.

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

Enligt punkt g avses med säkerhetsutredning av person en bedömning av den behöriga säkerhetsmyndigheten i enlighet med nationella lagar och bestämmelser, enligt vilken en fysisk person uppfyller villkoren för tillgång till och hantering av säkerhetsklassificerad information.

Enligt punkt h avses med säkerhetsutredning av företag en bedömning av den behöriga säkerhetsmyndigheten som i enlighet med nationella lagar och bestämmelser bekräftar att en juridisk person uppfyller villkoren för tillgång till och hantering av säkerhetsklassificerad information.

Artikel 3. *Behöriga säkerhetsmyndigheter* I punkt 1 anges vardera partens behöriga säkerhetsmyndigheter (National Security Authority, NSA) som ansvarar för det allmänna genomförandet av överenskommelsen. Behörig säkerhetsmyndighet i Finland är enligt 4 § i lagen om internationella förpliktelser som gäller informationssäkerhet utrikesministeriet, där uppgiften sköts av Nationella säkerhetsmyndigheten (NSA). I Ukraina har Ukrainas säkerhetstjänst (Security Service of Ukraine) utsetts till behörig säkerhetsmyndighet.

Enligt punkt 2 ska parterna underrätta varandra om de behöriga säkerhetsmyndigheter eller andra behöriga myndigheter (Competent Security Authorities, CSA) som till olika delar svarar för genomförandet av överenskommelsen. Utsedda säkerhetsmyndigheter (Designated Security Authority, DSA) i Finland är enligt 4 § i lagen om internationella förpliktelser som gäller informationssäkerhet försvarsministeriet, huvudstaben, skyddspolisen och Transport- och kommunikationsverket.

Enligt punkt 3 ska parterna underrätta varandra om eventuella senare ändringar i de behöriga säkerhetsmyndigheterna.

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

I punkt 2 definieras hur Finlands och Ukrainas säkerhetsklasser motsvarar varandra. Den högsta säkerhetsklassen, som kräver de strängaste informationssäkerhetsåtgärderna, är ”ERITTÄIN SALAINEN / YTTERST HEMLIG" (Особливої важливості). Till denna kategori räknas i Finland information som, om den obehö-

rigen röjs eller obehörigen används, kan orsaka särskilt påtaglig skada för försvaret, beredskapen inför undantagsförhållanden, internationella relationer, brottsbekämpningen, den allmänna säkerheten, en fungerande stats- och samhällsekonomi eller på något annat jämförbart sätt skada för Finlands säkerhet. Den näst högsta säkerhetsklassen är ”SALAINEN / HEMLIG” (Цілком таємно). Hit hör i Finland information som, om den obehörigen röjs eller obehörigen används, kan orsaka betydande skada för försvaret, beredskapen inför undantagsförhållanden, internationella relationer, brottsbekämpningen, den allmänna säkerheten, en fungerande stats- och samhällsekonomi eller på något annat jämförbart sätt skada för Finlands säkerhet. Den tredje högsta säkerhetsklassen är ”LUOTTAMUKSELLINEN / KONFIDENTIELL” (Таємно). Med den avses i Finland information som, om den obehörigen röjs eller obehörigen används, kan orsaka skada för försvaret, beredskapen inför undantagsförhållanden, internationella relationer, brottsbekämpningen, den allmänna säkerheten, en fungerande stats- och samhällsekonomi eller på något annat jämförbart sätt skada för Finlands säkerhet. Till den fjärde säkerhetsklassen ”KÄYTTÖ RAJOITETTU / BEGRÄNSAD TILLGÅNG” (Для службового користування) hör information som, om den obehörigen röjs eller obehörigen används, kan orsaka lindrig skada för försvaret, beredskapen inför undantagsförhållanden, internationella relationer, brottsbekämpningen, den allmänna säkerheten, en fungerande stats- och samhällsekonomi eller på något annat jämförbart sätt skada för Finlands säkerhet.

Finlands internationella relationer skyddas i 24 § 1 mom. 1 och 2 punkten i offentlighetslagen, försvaret i 10 punkten och säkerheten i 5, 8 och 9 punkten i samma moment. Andra allmänna intressen som avses i offentlighetslagen kan till exempel vara skyddet av säkerhetsarrangemangen för statsledningen och statsbesök och för datasystem (24 § 1 mom. 7 punkten) samt samhällsekonomin (24 § 1 mom. 11 och 12 punkten). Allmänt tillämpliga bestämmelser om sekretess- och klassificeringsanteckningar i myndighetshandlingar ingår i 25 § i offentlighetslagen. Enligt 25 § 3 mom. finns bestämmelser om anteckning av säkerhetsklass i lagen om informationshantering inom den offentliga förvaltningen.

Enligt 18 § 1 mom. i lagen om informationshantering inom den offentliga förvaltningen ska myndigheter vid statliga ämbetsverk och inrättningar, domstolar och nämnder som har inrättats för att behandla besvärsärenden säkerhetsklassificera handlingar och förse dem med anteckning om säkerhetsklass som visar vilket slag av informationssäkerhetsåtgärder som ska vidtas vid behandlingen av dem. Anteckningen om säkerhetsklass ska göras om handlingen eller informationen i den är sekretessbelagd enligt 24 § 1 mom. 2, 5 eller 7–11 punkten i offentlighetslagen och om obehörigt röjande eller obehörig användning av handlingen kan orsaka skada för försvaret, beredskapen inför undantagsförhållanden, internationella relationer, brottsbekämpningen, den allmänna säkerheten, en fungerande stats- och samhällsekonomi eller på något annat jämförbart sätt skada för Finlands säkerhet. Enligt 18 § 2 mom. i informationshanteringslagen får en handling inte förses med en anteckning om säkerhetsklass i andra fall än sådana som avses i 1 mom., om anteckningen inte behövs för att fullgöra en internationell förpliktelse som gäller informationssäkerhet eller om handlingen annars har samband med internationellt samarbete.

Enligt 18 § 3 mom. i informationshanteringslagen ska sådana handlingar som avses i lagen om internationella förpliktelser som gäller informationssäkerhet förses med anteckning om säkerhetsklass så som föreskrivs i den lagen. Enligt 8 § i lagen om internationella förpliktelser som gäller informationssäkerhet ska särskilt känsligt informationsmaterial oberoende av vad som föreskrivs i lagen om informationshantering inom den offentliga förvaltningen 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. Enligt 18 § 4 mom. i informationshanteringslagen finns det bestämmelser om säkerhetsklassificering, anteckningar i säkerhetsklassificerade handlingar och informationssäkerhetsåtgärder som anknyter till behandlingen av säkerhetsklassificerade handlingar i statsrådets förordning om säkerhetsklassificering av handlingar inom statsförvaltningen.

Specialbestämmelser om säkerhetsklassificering och märkning av säkerhetsklass finns i 3 § i säkerhetsklassificeringsförordningen och om säkerhetsklassificeringens motsvarighet vid tillgodoseende av internationella

förpliktelser som gäller informationssäkerheten i förordningens 4 §. Specialbestämmelser om säkerhetsklassificeringsmärkning på svenska finns i förordningens 3 § 3 mom.

Enligt punkt 3 i artikeln ska den mottagande parten säkerställa att säkerhetsklassificeringar inte ändras eller upphävs utan skriftligt tillstånd av den utlämnande parten.

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

Enligt punkt 1 ska parterna vidta alla lämpliga åtgärder i enlighet med sina nationella lagar och bestämmelser för att skydda sådan säkerhetsklassificerad information som avses i överenskommelsen. Parterna ska enligt samma punkt ge denna information åtminstone samma skyddsnivå som 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 får tillgång till säkerhetsklassificerad information endast ges personer som har ett informationsbehov och som vid behov har säkerhetsklarerats i enlighet med nationella lagar och bestämmelser och bemyndigats att få tillgång till sådan information, såväl som instruerats om sitt ansvar i skyddet av säkerhetsklassificerad information. Säkerhetsutredning krävs inte av personer som på grund av sina uppgifter annars på behörigt sätt getts tillgång till sådan information i enlighet med nationella lagar och bestämmelser.

Enligt punkt 4 krävs ingen säkerhetsutredning av person för tillgång till säkerhetsklassificerad information i säkerhetsklass KÄYTTÖ RAJOITETTU / BEGRÄNSAD TILLGÅNG eller Для службового користування.

Enligt punkt 5 får säkerhetsklassificerad information användas endast för det ändamål för vilket det har lämnats ut. En bestämmelse som motsvarar denna förpliktelse finns i 6 § 2 mom. i lagen om internationella förpliktelser som gäller informationssäkerhet.

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

Artikel 6. *Säkerhetsklassificerade kontrakt*. Artikeln innehåller bestämmelser om ingående av sådana säkerhetsklassificerade kontrakt inom någondera partens territorium som avses i artikel 2 led b.

Enligt punkt 1 ska den mottagande partens behöriga säkerhetsmyndighet på begäran meddela den utlämnande partens behöriga säkerhetsmyndighet huruvida en föreslagen kontraktspart, som deltar i förhandlingar som föregår säkerhetsklassificerade kontrakt eller i genomförandet av ett sådant kontrakt, har beviljats intyg över säkerhetsutredning av person eller av företag i den säkerhetsklass som krävs. Om en kontraktspart inte har något sådant intyg, får den utlämnande partens behöriga säkerhetsmyndighet be den mottagande partens behöriga säkerhetsmyndighet säkerhetsklarera kontraktsparten.

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

Enligt punkt 3 krävs ingen säkerhetsutredning av företag för tillgång till säkerhetsklassificerad information i säkerhetsklass KÄYTTÖ RAJOITETTU / BEGRÄNSAD TILLGÅNG eller Для службового користування.

Enligt punkt 4 ska ett säkerhetsklassificerat kontrakt, för att säkerheten ska kunna övervakas och kontrolleras i tillräcklig utsträckning, innehålla anvisningar om säkerhetsklassificering och tillämpliga säkerhetsföreskrifter i enlighet med bilaga 1. En kopia av dessa säkerhetsföreskrifter ska tillställas den partens behöriga säkerhetsmyndigheter inom vars jurisdiktion det säkerhetsklassificerade kontraktet ska genomföras.

Enligt punkt 5 får företrädare för parternas behöriga säkerhetsmyndigheter besöka varandra för att bedöma effekten av de åtgärder som en kontraktspart har vidtagit för att skydda säkerhetsklassificerad information med anknytning till ett säkerhetsklassificerat kontrakt. Bestämmelsen har också samband med artikel 10.2 i överenskommelsen där det bestäms om besök av parternas säkerhetsmyndigheter.

De nationella bestämmelserna om säkerhetsklassificerade kontrakt finns i lagen om internationella förpliktelser som gäller informationssäkerhet 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 i 18 § 2 mom. (besök av representanter för internationella organ och för fördragsslutande stater). I 18 § 2 mom. i lagen om internationella förpliktelser som gäller informationssäkerhet föreskrivs 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 att dessa företag ska ge den behöriga myndigheten en förbindelse om att de bevarar sin informationssäkerhetsnivå och ger myndigheten tillstånd att komma in i sina 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 i icke-elektronisk form.

Enligt punkt 1 ska den utlämnande parten och den mottagande parten förmedla säkerhetsklassificerad information till varandra genom mellanstatliga, diplomatiska och officiella kanaler eller på något annat sätt som avtalas mellan deras behöriga säkerhetsmyndigheter.

Enligt punkt 2 ska den utlämnande parten och den mottagande parten förmedla säkerhetsklassificerad information till varandra på elektronisk väg endast på ett sådant säkert sätt som har avtalats mellan de behöriga säkerhetsmyndigheterna.

Bestämmelserna i artikeln är i samklang med säkerhetsklassificeringsförordningens 13 § om transport av en handling, informationshanteringslagens 14 § om informationsöverföring i datanät och säkerhetsklassificeringsförordningens 12 § om överföring av en handling via datanätet.

Artikel 8. *Översättning, kopiering och utplåning av säkerhetsklassificerad information.* Enligt punkt 1 ska alla översättningar och kopior av säkerhetsklassificerad information förses med anteckning om tillämplig säkerhetsklass och skyddas på samma sätt som den ursprungliga säkerhetsklassificerade informationen. 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 information i säkerhetsklass ERITTÄIN SALAINEN / YTTERST HEMLIG eller Особливої важливості översättas eller kopieras endast med skriftligt samtycke av den utlämnande parten.

Enligt punkt 4 ska information i säkerhetsklass ERITTÄIN SALAINEN / YTTERST HEMLIG eller Особливої важливості återlämnas till den utlämnande parten, om inte annat avtalas.

Enligt punkt 5 ska information i säkerhetsklass SALAINEN / HEMLIG eller Цілком таємно eller lägre utplånas när den mottagande parten anser att den inte längre behövs, i enlighet med den mottagande partens nationella lagar och bestämmelser.

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

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

Artikel 9. *Besök*
Enligt punkt 1 krävs det för besök som inbegriper tillgång till säkerhetsklassificerad information i säkerhetsklass LUOTTAMUKSELLINEN / KONFIDENTIELL eller Таємно eller högre skriftligt förhandstillstånd av värdpartens behöriga säkerhetsmyndighet. Enligt punkt 1 led a–b ska besökare få tillgång till säkerhetsklassificerad information endast, om den behöriga säkerhetsmyndigheten hos den part som sänder besökare har gett dem det begärda besökstillståndet eller de begärda besökstillstånden, och de har utfärdats ett relevant intyg över säkerhetsutredning av person.

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

Enligt punkt 3 ska tillstånd för upprepade besök gälla i högst 12 månader.

Artikel 10. *Säkerhetssamarbete.* Artikeln innehåller en bestämmelse om säkerhetssamarbetet mellan de behöriga säkerhetsmyndigheterna.

Enligt punkt 1 ska de behöriga säkerhetsmyndigheterna i syfte att genomföra överenskommelsen underrätta 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 på begäran informera varandra om sina nationella säkerhetsnormer, förfaranden och tillämpningar för skyddet av säkerhetsklassificerad information. För detta ändamål kan de behöriga säkerhetsmyndigheterna besöka varandra. Bestämmelser om besök finns i 18 § i lagen om internationella förpliktelser som gäller informationssäkerhet.

Enligt punkt 3 ska de behöriga säkerhetsmyndigheterna på begäran bistå varandra i enlighet med nationella lagar och bestämmelser vid utarbetandet av säkerhetsutredningar. 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 motsvarar kraven i den nationella lagstiftningen.

Enligt punkt 4 ska de behöriga säkerhetsmyndigheterna utan dröjsmål underrätta varandra om ändringar i aktuella intyg över säkerhetsutredning av personer och företag.

Artikel 11. *Kränkning av dataskyddet.* Enligt punkt 1 ska vardera parten utan dröjsmål underrätta den andra parten om misstänkta eller upptäckta kränkningar av dataskyddet som rör säkerhetsklassificerad information.

Enligt punkt 2 ska den part som har jurisdiktion utan dröjsmål undersöka fallet. Den andra parten ska vid behov samarbeta i undersökningen.

Enligt punkt 3 ska den part som har jurisdiktion vidta alla möjliga tillämpliga åtgärder i enlighet med sina nationella lagar och bestämmelser för att begränsa följderna av en dataskyddskränkning och för att förebygga ytterligare kränkningar. Den andra parten ska informeras om utfallet av utredningen och om vidtagna åtgärder.

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 enligt överenskommelsen.

Artikel 13. *Tvistlösning. Enligt artikeln ska tvister mellan parterna om tolkning eller tillämpning av överenskommelsen avgöras i samråd mellan parterna.*

Artikel 14. *Slutbestämmelser.* Artikeln innehåller bestämmelser om ikraftträdande, ändring, uppsägning, förpliktelser till följd av uppsägning och om deponering av överenskommelsen för registrering hos Förenta nationernas sekretariat i överensstämmelse med artikel 102 i Förenta nationernas stadga. Enligt artikeln ska överenskommelsen gälla tills vidare. Överenskommelsen kan ändras på gemensam skriftlig överenskommelse mellan parterna. En part får säga upp överenskommelsen genom skriftlig underrättelse till den andra parten via diplomatiska kanaler iakttagande en uppsägningstid på sex (6) månader. Om överenskommelsen sägs upp med stöd av artikeln i fråga, 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.

8 Ikraftträdande

Enligt artikel 14.1 i överenskommelsen ska parterna underrätta varandra när de nationella åtgärder som krävs för ikraftträdandet av överenskommelsen har slutförts. Överenskommelsen träder i kraft den första dagen i den andra månaden efter att den senare underrättelsen har tagits emot.

Det föreslås att den lag som ingår i propositionen ska träda i kraft samtidigt som överenskommelsen träder i kraft för Finlands del, vid en tidpunkt som föreskrivs genom förordning av statsrådet.

9 Bifall av Ålands lagting

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).

10 Behovet av riksdagens samtycke och behandlingsordning

10.1 Behovet av riksdagens samtycke

Enligt 94 § 1 mom. i grundlagen godkänner riksdagen fördrag och andra internationella förpliktelser som innehåller sådana bestämmelser som hör till området för lagstiftningen. Enligt grundlagsutskottets tolkningspraxis ska en bestämmelse anses höra till området för lagstiftningen om den gäller utövande eller begränsning av någon grundläggande fri- eller rättighet som är skyddad i grundlagen, om den i övrigt gäller grunderna för individens rättigheter och skyldigheter, om den sak som bestämmelsen gäller är sådan att om den enligt grundlagen ska föreskrivas i lag eller om det finns lagbestämmelser om den sak som bestämmelsen gäller eller om det enligt rådande uppfattning i Finland ska lagstiftas om saken. Grundlagsutskottet har ansett att en bestämmelse i en internationell förpliktelse på dessa grunder hör till området för lagstiftningen oavsett om den strider mot eller överensstämmer med en lagbestämmelse i Finland (se exempelvis 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 definieras bland annat vad som avses med säkerhetsklassificerad information, säkerhetsklassificerat kontrakt, säkerhetsutredningar och kränkning av dataskyddet. Eftersom dessa definitioner antingen direkt eller indirekt påverkar tolkningen och tillämpningen av sådana materiella bestämmelser i överenskommelsen som hör till området för lagstiftningen kräver de riksdagens godkännande (GrUU 6/2001 rd och GrUU 24/2001 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 konstaterande och har därför inte ansetts kräva riksdagens samtycke.

Artikel 4 innehåller bestämmelser om anteckningar om säkerhetsklassificering och om säkerhetsklassernas motsvarighet. De allmänt tillämpliga bestämmelserna om anteckning om sekretess och klassificering finns i 25 § i offentlighetslagen. Enligt den ska det göras en sekretessanteckning i en myndighetshandling som en myndighet ger ut till en part och som ska vara sekretessbelagd på grund av någon annans eller allmänt intresse. I andra sekretessbelagda handlingar kan en anteckning göras efter prövning. I 18 § i lagen om informationshantering finns det särskilda bestämmelser om anteckning om säkerhetsklass och i 8 § i lagen om internationella förpliktelser som gäller informationssäkerhet bestämmelser om anteckning om säkerhetsklass i fråga om särskilt känsligt informationsmaterial. Enligt den ska särskilt känsligt informationsmaterial oberoende av vad som föreskrivs i lagen om informationshantering inom den offentliga förvaltningen 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 om åtgärder som krävs för att skydda säkerhetsklassificerad information inom tillämpningsområdet för överenskommelsen och som begränsar utlämnande, förmedling och användning av samt tillgången till informationen. Artikel 5.2 utgör kärnan i överenskommelsen, enligt vilken parterna inte ger tredje parter tillgång till säkerhetsklassificerad information utan den utlämnande partens skriftliga förhandssamtycke och utifrån vilken Finland kan skydda säkerhetsklassificerad information som utbyts med stöd av överenskommelsen utan den skaderekvisitbedömning som föreskrivs i offentlighetslagen. I Finland är myndighetshandlingar enligt huvudregeln offentliga. Var och en har enligt 12 § 2 mom. i grundlagen rätt att ta del av myndigheters offentliga handlingar 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 och 5.4 anges också en begränsning med avseende på personer som ska få tillgång till säkerhetsklassificerad information. I

artikel 5.3 i överenskommelsen föreskrivs ytterligare om parternas skyldighet att i förekommande fall låta utföra en säkerhetsutredning över personer som har bemyndigats tillgång till säkerhetsklassificerad information som avses i denna punkt. I upplägget för säkerhetsutredningar ska det som sägs i 10 § 1 mom. i grundlagen om tryggat privatliv och om plikten att lagstifta om skydd för personuppgifter beaktas. I Finland finns det i säkerhetsutredningslagen föreskrifter om vilka personer som är föremål för säkerhetsutredningar och om utredningsförfarandet. Bestämmelsen hör följaktligen till området för lagstiftningen och kräver riksdagens samtycke för att träda i kraft. Enligt artikel 5.5 får säkerhetsklassificerad information användas endast för det ändamål för vilket det har lämnats ut. En motsvarande bestämmelse finns i 6 § 2 mom. i lagen om internationella förpliktelser som gäller informationssäkerhet. Bestämmelsen i denna punkt hör följaktligen till området för lagstiftningen.

I artikel 6 i överenskommelsen finns det bestämmelser om säkerhetsklassificerade kontrakt och om säkerhetsutredning av företag som ingår sådana kontrakt samt om rätten för representanter för parternas behöriga säkerhetsmyndigheter att besöka varandra för att bedöma effekten av de åtgärder som en kontraktspart har vidtagit för att skydda säkerhetsklassificerad information i anknytning till ett säkerhetsklassificerat kontrakt. 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. Syftet med besök mellan avtalsparternas representanter är att säkerställa att överenskommelsens syfte om ett korrekt skydd för säkerhetsklassificerad information förverkligas. Denna besöksrätt innehåller inget sådant utövande av offentlig makt eller sådan granskningsrätt som står i konflikt med grundlagen (GrUU 39/1997 rd). I 18 § i lagen om internationella förpliktelser som gäller informationssäkerhet finns motsvarande bestämmelser om omständigheter i anknytning till genomförande av avtalsbestämmelser som gäller besök. Bestämmelserna om säkerhetsklassificerade kontrakt, om intyg över företagssäkerhet och om besök av representanter för den andra fördragsstaten hör följaktligen till området för lagstiftningen.

I artikel 11 i överenskommelsen förutsätts det att de behöriga 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 fallet. Vidare ska enligt samma artikel den part som har jurisdiktion vidta alla möjliga tillämpliga åtgärder i enlighet med sina nationella lagar och bestämmelser för att begränsa följderna av en dataskyddskränkning och för att förebygga ytterligare kränkningar. Den andra parten ska informeras om utfallet av utredningen och om vidtagna åtgärder. I 19 § i lagen om internationella förpliktelser som gäller informationssäkerhet föreskrivs om de nationella säkerhetsmyndigheternas skyldigheter i sådana situationer som avses i bestämmelserna i överenskommelsen. Följaktligen hör bestämmelserna i artikeln till området för lagstiftningen.

10.2 Behandlingsordning

Allmänt tillämpliga bestämmelser om sekretess avseende säkerhetsklassificerade uppgifter finns i lagen om internationella förpliktelser som gäller informationssäkerhet. Enligt 6 § 1 mom. i den lagen ska särskilt känsligt informationsmaterial sekretessbeläggas, om inte annat följer av en internationell förpliktelse som gäller informationssäkerhet. Enligt 6 § 2 mom. får särskilt känsligt informationsmaterial användas och lämnas ut endast för angivet ändamål, om inte den som bestämt materialets säkerhetsklass har samtyckt till något annat. 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 informationssäkerhet. 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 Ukraina 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.

Kläm 1

Med stöd av vad som anförts ovan och i enlighet med 94 § i grundlagen föreslås det att riksdagen godkänner den i Kiev den 12 september 2019 mellan republiken Finland och Ukraina ingångna överenskommelsen om ömsesidigt skydd av säkerhetsklassificerad information.

Kläm 2

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

Lagförslag

Lag

om överenskommelsen med Ukraina om ömsesidigt skydd av säkerhetsklassificerad information

I enlighet med riksdagens beslut föreskrivs:

1 §

De bestämmelser som hör till området för lagstiftningen i den i Kiev den 12 september 2019 mellan Republiken Finland och Ukraina ingångna överenskommelsen om ömsesidigt 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 29 oktober 2020

Statsminister

Sanna Marin

Utrikesminister Pekka Haavisto

Fördragstext

ÖVERENSKOMMELSE MELLAN REPUBLIKEN FINLAND OCH UKRAINA OM ÖMSESIDIGT SKYDD AV SÄKERHETSKLASSIFICERAD INFORMATION

Republiken Finland och Ukraina, nedan kallade ”parterna”, har

för att skydda säkerhetsklassificerad information som särskilt rör utrikesärenden, försvar, säkerhet, brottsbekämpande, vetenskapliga och tekniska frågor eller frågor som rör näringslivet och som utbyts mellan parterna eller mellan offentlig- eller privaträttsliga juridiska eller fysiska personer inom deras jurisdiktion som hanterar säkerhetsklassificerad information,

kommit överens om följande:

Artikel 1

Syfte och tillämpningsområde

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

Artikel 2

Definitioner

I denna överenskommelse avses med
a) *säkerhetsklassificerad information* information, handlingar eller material, oavsett form, som har säkerhetsklassificerats och försetts med klassificeringsanteckning i enlighet med nationella lagar och bestämmelser, såväl som information, handlingar eller material som har framställts utifrån sådan säkerhetsklassificerad information och försetts med tillämplig klassificeringsanteckning,

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

The Republic of Finland and Ukraine, hereinafter referred to as “the Parties”,

In order to protect Classified Information related especially to foreign affairs, defence, security, law enforcement, scientific, industrial and technological matters exchanged between the Parties, or public or private legal entities or individuals that handle Classified Information under the jurisdiction of the Parties,

have agreed as follows:

Article 1

Purpose and scope of application

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

Article 2

Definitions

For the purposes of this Agreement:
a) *Classified Information* means any information, document or material of whatever form, to which a security classification level has been applied and which has been marked in accordance with national laws and regulations, as well as any information, document or material that has been generated on the basis of such Classified Information and marked accordingly;

b) *säkerhetsklassificerat kontrakt* kontrakt eller underleverantörskontrakt som innehåller eller som har anknytning till säkerhetsklassificerad information,
c) *utlämnande part* part som lämnar ut säkerhetsklassificerad information till den mottagande parten,
d) *mottagande part* part och offentligrättsliga eller privaträttsliga juridiska eller fysiska personer inom partens jurisdiktion till vilken den utlämnande parten lämnar ut säkerhetsklassificerad information,
e) *behörig säkerhetsmyndighet* nationell säkerhetsmyndighet eller särskilt utsett statligt organ som i enlighet med parternas nationella lagar och bestämmelser har bemyndigats att svara för genomförandet av denna överenskommelse,
f) *kränkning av dataskyddet* en gärning eller försummelse i strid med nationella lagar och bestämmelser som kan medföra att säkerhetsklassificerad information går förlorad eller äventyras,
g) *säkerhetsutredning av person* en bedömning av den behöriga säkerhetsmyndigheten i enlighet med nationella lagar och bestämmelser, enligt vilken en fysisk person uppfyller villkoren för tillgång till och hantering av säkerhetsklassificerad information,
h) *säkerhetsutredning av företag* en bedömning av den behöriga säkerhetsmyndigheten som i enlighet med nationella lagar och bestämmelser bekräftar att en juridisk person uppfyller villkoren för tillgång till och hantering av säkerhetsklassificerad information,
i) *kontraktspart* juridisk eller fysisk person som har rättskapacitet att ingå kontrakt.

Artikel 3

Behöriga säkerhetsmyndigheter

1. Parterna har utsett följande behöriga säkerhetsmyndigheter att svara för det allmänna genomförandet av denna överenskommelse:

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 to the Recipient Party,
d) *Recipient Party* means the Party, as well as any public or private 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 or a specially designated state body authorised in accordance with the national laws and regulations of the Parties which is responsible for the implementation of this Agreement;
f) *Breach of Security* means an act or an omission contrary to national laws and regulations which may lead to the loss or compromise of Classified Information;

g) *Personnel Security Clearance (PSC)* means determination by the Competent Security Authority confirming in accordance with its national laws and regulations, that an individual is eligible to have access to and to handle Classified Information;
h) *Facility Security Clearance (FSC)* means determination by the Competent Security Authority confirming in accordance with its national laws and regulations, that a legal entity is eligible to have access to and to handle Classified Information;
i) *Contractor* means an individual or legal entity possessing the legal capacity to undertake contracts.

Article 3

Competent Security Authorities

1. The Competent Security Authorities designated by the Parties as responsible for the general implementation of this Agreement are:

I Republiken Finland	I Ukraina
Nationella säkerhetsmyndigheten ***Utrikesministeriet*** ***FINLAND***	***Security Service of Ukraine***

In the Republic of Finland	In Ukraine
National Security Authority (NSA) ***Ministry for Foreign Affairs*** ***FINLAND***	***Security Service of Ukraine***

2. Parterna ska underrätta varandra om de behöriga säkerhetsmyndigheter eller andra behöriga myndigheter som till olika delar svarar för genomförandet av denna överenskommelse.

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

2. The Parties shall notify each other of any Competent Security Authorities or other competent authorities, which shall be responsible for the implementa-tion of aspects of this Agreement.

3. The Parties shall notify each other of any subsequent changes of the Com-petent Security Authorities.

Artikel 4

Säkerhetsklasser

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

2. Säkerhetsklasserna motsvarar varandra enligt följande:

Article 4

Security classifications

1. Any Classified Information provid-ed under this Agreement shall be marked with the appropriate security classification in accordance with nation-al laws and regulations.

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

Republiken Finland	Ukraina	Motsvarighet på engelska
ERITTÄIN SALAINEN eller YTTERST HEMLIG	Особливої важливості	top secret
SALAINEN eller HEMLIG	Цілком таємно	secret

LUOTTAMUKSELLINEN eller KONFIDENTIELL	Таємно	confidential
KÄYTTÖ RAJOITETTU eller BEGRÄNSAD TILLGÅNG	Для службового користування	restricted

The Republic of Finland	**Ukraine**	**English translation**
ERITTÄIN SALAINEN eller YTTERST HEMLIG	Особливої важливості	top secret
SALAINEN eller HEMLIG	Цілком таємно	secret
LUOTTAMUKSELLINEN eller KONFIDENTIELL	Таємно	confidential
BEGRÄNSAD TILLGÅNG eller BEGRÄNSAD TILLGÅNG	Для службового користування	restricted

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

Artikel 5

Skydd av säkerhetsklassificerad information

1. Parterna ska vidta alla lämpliga åtgärder i enlighet med sina nationella lagar och bestämmelser för att skydda sådan säkerhetsklassificerad information som avses i denna överenskommelse. De ska ge denna information åtminstone samma skyddsnivå som egen information i motsvarande säkerhetsklass.

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

Article 5

Protection of Classified Information

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

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

3. Tillgång till säkerhetsklassificerad information får endast ges personer som har ett informationsbehov och som vid behov har säkerhetsklarerats i enlighet med nationella lagar och bestämmelser och bemyndigats att få tillgång till sådan information, såväl som instruerats om sitt ansvar i skyddet av säkerhetsklassificerad information. Säkerhetsutredning krävs inte av personer som på grund av sina uppgifter annars på behörigt sätt getts tillgång till sådan information i enlighet med nationella lagar och bestämmelser.

4. Det krävs ingen säkerhetsutredning av person för tillgång till säkerhetsklassificerad information i säkerhetsklass KÄYTTÖ RAJOITETTU / BEGRÄNSAD TILLGÅNG eller Для службового користування.

5. Säkerhetsklassificerad information får användas endast för det ändamål för vilket det har lämnats ut.

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 national laws and regulations, have been security cleared, where appropriate, and authorised to have access to such information as well as briefed on their responsibilities for the protection of Classified Information. The security clearance is not required if persons are otherwise duly authorised by virtue of their functions in accordance with national laws and regulations.

4. A Personnel Security Clearance is not required for access to Classified Information at the level KÄYTTÖ RAJOITETTU/BEGRÄNSAD TILLGÅNG /«Для службового користування»

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

Artikel 6

Säkerhetsklassificerade kontrakt

1. Den mottagande partens behöriga säkerhetsmyndighet ska på begäran meddela den utlämnande partens behöriga säkerhetsmyndighet huruvida en föreslagen kontraktspart, som deltar i förhandlingar som föregår säkerhetsklassificerade kontrakt eller i genomförandet av ett sådant kontrakt, har beviljats intyg över säkerhetsutredning av person eller av företag i den säkerhetsklass som krävs. Om en kontraktspart inte har något sådant intyg, får den utlämnande partens behöriga säkerhetsmyndighet be den mottagande partens behöriga säkerhetsmyndighet säkerhetsklarera kontraktsparten.

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

Article 6

Classified Contracts

1. Upon request, the Competent Security Authority of the Recipient Party 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 FSC orPSCcorresponding 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 Party.

2. In the case of an open tender the Competent Security Authority of the Recipient Party may provide the Competent Security Authority of the Originating Party with the relevant FSC or PSC certificates without a formal request.

3. Det krävs ingen säkerhetsutredning av företag för tillgång till säkerhetsklassificerad information i säkerhetsklass KÄYTTÖ RAJOITETTU / BEGRÄNSAD TILLGÅNG eller Для службового користування.

4. För att säkerheten ska kunna övervakas och kontrolleras i tillräcklig utsträckning ska ett säkerhetsklassificerat kontrakt innehålla anvisningar om säkerhetsklassificering och tillämpliga säkerhetsföreskrifter i enlighet med bilaga 1. En kopia av dessa säkerhetsföreskrifter ska tillställas den partens behöriga säkerhetsmyndigheter inom vars jurisdiktion det säkerhetsklassificerade kontraktet ska genomföras.

5. Företrädare för parternas behöriga säkerhetsmyndigheter får besöka varandra för att bedöma effekten av de åtgärder som en kontraktspart har vidtagit för att skydda säkerhetsklassificerad information med anknytning till ett säkerhetsklassificerat kontrakt.

Artikel 7

Förmedling av säkerhetsklassificerad information

1. Den utlämnande parten och den mottagande parten ska förmedla säkerhetsklassificerad information till varandra genom mellanstatliga, diplomatiska och officiella kanaler eller på något annat sätt som avtalas mellan deras behöriga säkerhetsmyndigheter.

2. Den utlämnande parten och den mottagande parten ska förmedla säkerhetsklassificerad information till varandra på elektronisk väg endast på ett sådant säkert sätt som har avtalats mellan de behöriga säkerhetsmyndigheterna.

Artikel 8

Översättning, kopiering och utplåning av säkerhetsklassificerad information

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

3. A Facility Security Clearance is not required for Classified Contracts at the level KÄYTTÖ RAJOITETTU/BEGRÄNSAD TILLGÅNG /«Для службового користування»

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

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

Article 7

Transmission of Classified Information

1. Classified Information shall be transmitted between the Originating Party and the Recipient Party through government-to-government, diplomatic and official channels or as otherwise agreed by their Competent Security Authorities.

2. Classified Information shall be transmitted between the Originating Party and the Recipient Party electronically only by secure means agreed between the competent authorities.

Article 8

Translation, reproduction and destruction of Classified Information

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

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

3. Information i säkerhetsklass ERITTÄIN SALAINEN / YTTERST HEMLIG eller Особливої важливості får översättas eller kopieras endast med skriftligt samtycke av den utlämnande parten.

4. Information i säkerhetsklass ERITTÄIN SALAINEN / YTTERST HEMLIG eller Особливої важливості ska återlämnas till den utlämnande parten, om inte annat avtalas.

5. Information i säkerhetsklass SALAINEN / HEMLIG eller Цілком таємно eller lägre ska utplånas när den mottagande parten anser att den inte längre behövs, i enlighet med den mottagande partens 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 omedelbart utplånas. Den mottagande parten ska så snart 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 Таємно eller högre krävs skriftligt förhandstillstånd av värdpartens behöriga säkerhetsmyndighet. Besökare ska få tillgång till säkerhetsklassificerad information endast, om

a) den behöriga säkerhetsmyndigheten hos den part som sänder besökare har gett dem det begärda besökstillståndet eller de begärda besökstillstånden, och

b) de har utfärdats ett relevant intyg över säkerhetsutredning av person.

2. Den berörda behöriga säkerhetsmyndigheten hos den part som föreslår besöket ska

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 at the level ERITTÄIN SALAINEN/ YTTERST HEMLIGor “Особливої важливості”, shall be translated or reproduced only upon the written consent of the Originating Party.

4. Classified Information at the level ERITTÄIN SALAINEN/ YTTERST HEMLIG or /“Особливої важливості” shall be returned to the Originating Party unless otherwise agreed.

5. Classified Information at the level SALAINEN/HEMLIG or “Цілком таємно”or lower 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 Party 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 the level LUOTTAMUKSELLINEN/KONFIDENTIELL or “Таємно” or above require prior written authorisation 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 Security Clearance.

2. The relevant Competent Security Authority of the requesting Party shall notify the relevant Competent Security Authority of the

underrätta värdpartens berörda behöriga säkerhetsmyndighet om det planerade besöket och se till att den myndigheten får besöksbegäran minst 14 dagar före den planerade tidpunkten för besöket. I brådskande fall kan de behöriga säkerhetsmyndigheterna komma överens om en kortare tidsfrist. En besöksbegäran ska innehålla de uppgifter som anges i bilaga 2 till denna överenskommelse.

3. Tillstånd för upprepade besök ska gälla i högst 12 månader.

host Party of the planned visit, 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.

Artikel 10

Säkerhetssamarbete

1. I syfte att genomföra denna överenskommelse ska de behöriga säkerhetsmyndigheterna underrätta 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 denna överenskommelse ska de behöriga säkerhetsmyndigheterna samråda sinsemellan. De ska på begäran informera varandra om sina nationella säkerhetsnormer, förfaranden och tillämpningar för skyddet av säkerhetsklassificerad information. För detta ändamål kan de behöriga säkerhetsmyndigheterna besöka varandra.

3. De behöriga säkerhetsmyndigheterna ska på begäran bistå varandra i enlighet med nationella lagar och bestämmelser vid utarbetandet av säkerhetsutredningar av personer och företag.

4. De behöriga säkerhetsmyndigheterna ska utan dröjsmål underrätta varandra om ändringar i aktuella intyg över säkerhetsutredning av personer och företag.

Article 10

Security co-operation

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

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

4. The Competent Security Authorities shall promptly inform each other about changes in relevant PSC and FSC certificates.

Artikel 11

Kränkning av dataskyddet

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

Article 11

Breach of Security

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

2. Den part som har jurisdiktion ska utan dröjsmål undersöka fallet. Den andra parten ska vid behov samarbeta i undersökningen.

3. Den part som har jurisdiktion ska vidta alla möjliga tillämpliga åtgärder i enlighet med sina nationella lagar och bestämmelser för att begränsa följderna av en dataskyddskränkning och för att förebygga ytterligare kränkningar. Den andra parten ska informeras om utfallet av utredningen och om vidtagna åtgärder.

2. The Party with jurisdiction shall investigate the incident 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 the Breach of Security and to prevent further Breaches of Security. 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 enligt 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

Tvister mellan parterna om tolkning eller tillämpning av denna överenskommelse ska 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 by means of consultations between the Parties.

Artikel 14

Slutbestämmelser

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

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

3. En part får säga upp denna överenskommelse genom skriftlig underrättelse till den andra parten via diplomatiska kanaler iakttagande en uppsägningstid på sex (6) månader.

Article 14

Final provisions

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

2. This Agreement shall be in force for an indefinite period. 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.

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.

4. När denna överenskommelse har trätt i kraft ska den part inom vars territorium överenskommelsen har upprättats vidta omedelbara åtgärder för att få den registrerad i Förenta nationernas sekretariat i enlighet med artikel 102 i Förenta nationernas stadga. Den andra parten ska delges registreringen och registreringsnumret i Förenta nationernas fördragsserie så snart numret har tilldelats av Förenta nationernas sekretariat.

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.

4. After the entry into force of this Agreement, the Party in whose territory the Agreement is concluded shall take immediate measures so as to have the Agreement registered by the Secretariat of the United Nations in accordance with Article 102 of the UN Charter. The other Party shall be notified of the registration and of the registration number in the UN Treaty Series as soon as the UN Secretariat has issued it.

Till bekräftelse härav har representanter för parterna, därtill vederbörligen bemyndigade, undertecknat denna överenskommelse i
Kiev den 12 september 2019

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

In witness whereof the duly authorised representatives of the Parties have signed this Agreement,
in Kiev on the 12th day of September, 2019

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

FÖR REPUBLIKEN FINLAND

Päivi Laine

FÖR UKRAINA

Ivan Bakanov

FOR THE REPUBLIC OF FINLAND

Päivi Laine

FOR UKRAINE

Ivan Bakanov

Bilaga 1

Säkerhetsklassificerade kontrakt

Säkerhetsklassificerade kontrakt enligt artikel 6 i denna överenskommelse ska inbegripa säkerhetsklausuler med åtminstone följande uppgifter:

1. högsta tillämpliga säkerhetsklassificeringsnivå,
2. kontaktuppgifter till de berörda säkerhetsmyndigheter som ansvarar för genomförandet av överenskommelsen,
3. lagar och bestämmelser som gäller skydd av säkerhetsklassificerad information,
4. förfarandet och kraven för tillgång till säkerhetsklassificerad information,
5. hantering och lagring av säkerhetsklassificerad information,
6. överföring och elektronisk förmedling av säkerhetsklassificerad information,
7. märkning av säkerhetsklassificerad information,
8. skyddet av säkerhetsklassificerad information efter att ett kontrakt har löpt ut,
9. förstöring eller återlämnande av säkerhetsklassificerad information,
10. utlämnande av uppgifter om ett säkerhetsklassificerat kontrakt.

Annex 1

Classified Contracts

Classified Contracts referred to in Article 6 of this Agreement shall contain security clauses including at least the following:

1. the highest classification level applied;
2. contact details of the relevant security authorities responsible for implementing the contract;
3. laws and regulations concerning the protection of Classified Information;
4. procedure and requirements for access to Classified Information;
5. handling and storing of Classified Information;
6. transportation and electronic transmission of Classified Information;
7. marking of Classified Information;
8. protection of Classified Information after termination of the contract;
9. destroying or returning of Classified Information;
10. release of contract information.

Bilaga 2

Begäran om besök

En begäran om besök enligt artikel 9 i denna överenskommelse ska innehålla följande uppgifter:

1. besökarens efternamn, förnamn, födelseort, födelsetid och nationalitet, besökarens ställning med uppgift om den arbetsgivare besökaren företräder, uppgifter om det projekt som besökaren deltar i samt nummer på besökarens pass eller annan identitetshandling,
2. bekräftelse på att besökaren har en säkerhetsutredning av person 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 för det verksamhetsställe eller den anläggning som besöket gäller samt annan information av vikt för att fastställa om besöket eller besöken är motiverade,
6. datum, underskrift och stämpel/sigill av den sändande behöriga säkerhetsmyndigheten.

Annex 2

Request for visit

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

1. the visitor's family name, first name, place and date of birth 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 PSC 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.