

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

PROPOSITIONENS HUVUDSAKLIGA INNEHÅLL

I denna proposition föreslås det att riksdagen godkänner den i februari 2022 undertecknade överenskommelsen mellan Republiken Finland och Konungariket Nederländerna om utbyte och 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 säkerhetsklassificerad information som utbyts eller skapas i samarbetet mellan parterna. Det är fråga om sådant känsligt informationsmaterial som den utlämnande avtalsstaten särskilt har klassificerat till en nivå som kräver hög informationssäkerhet. Överenskommelsen förpliktar inte till utbyte av säkerhetsklassificerad information.

Parterna ska underrätta varandra när de nationella åtgärder som krävs för ikraftträdandet av överenskommelsen har vidtagits. 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

| | |
|---|----|
| PROPOSITIONENS HUVUDSAKLIGA INNEHÅLL | 1 |
| MOTIVERING | 3 |
| 1 Bakgrund och beredning | 3 |
| 1.1 Bakgrund | 3 |
| 1.2 Beredning | 4 |
| 2 Nuläge | 5 |
| 2.1 Lagen om internationella förpliktelser som gäller informationssäkerhet | 5 |
| 2.2 Säkerhetsutredningslagen | 7 |
| 3 Överenskommelsens syfte | 9 |
| 4 De viktigaste förslagen | 9 |
| 5 Propositionens konsekvenser | 9 |
| 5.1 Konsekvenser för medborgarna | 9 |
| 5.2 Konsekvenser för näringslivet | 10 |
| 5.3 Ekonomiska konsekvenser | 11 |
| 5.4 Konsekvenser för förvaltningen | 11 |
| 6 Remissvar | 11 |
| 7 Bestämmelserna i överenskommelsen och deras förhållande till lagstiftningen i Finland | 11 |
| 8 Motivering till lagförslaget | 19 |
| 9 Ikraftträdande | 20 |
| 10 Bifall av Ålands lagting | 20 |
| 11 Behovet av riksdagens samtycke samt behandlingsordning | 20 |
| 11.1 Behovet av riksdagens samtycke | 20 |
| 11.2 Behandlingsordning | 22 |
| LAGFÖRSLAG | 24 |
| Lag om överenskommelsen med Nederländerna om utbyte och ömsesidigt skydd av säkerhetsklassificerad information | 24 |
| FÖRDRAGSTEXT | 25 |

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 sedanvanligt 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 eller multilaterala 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)
- Det generella säkerhetsskyddsavtalet mellan Danmark, Finland, Island, Norge och Sverige (FördrS 10 och 12/2013)
- 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)
- Avtalet mellan Europeiska unionens medlemsstater (FördrS 76 och 77/2015)
- Österrike (FördrS 37 och 38/2018)
- Ungern (FördrS 63 och 64/2018)
- Belgien (FördrS 8 och 9/2022)

Det finns inte någon multilateral konvention inom området för informationssäkerhet. Ett undantag utgör det generella säkerhetsskyddsavtalet om ömsesidigt skydd och utbyte av säkerhetskyddsklassificerade 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. Syftet 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

Finland inledde ursprungligen förhandlingar med Nederländerna år 2007 för att få till en bilateral överenskommelse om ömsesidigt skydd av säkerhetsklassificerad information. Förhandlingarna avbröts på grund av hinder i anslutning till lagstiftningen i Nederländerna och inleddes på nytt år 2020. I den förhandlingsdelegation som statsrådet tillsatte den 27 augusti 2020 ingick företrädare för utrikesministeriet, transport- och kommunikationsverket, försvarsministeriet och Skyddspolisen. Delegationen leddes av Nationella säkerhetsmyndighetens chef Anu Laamanen från utrikesministeriet. Förhandlingarna med Nederländerna avslutades den 18 juni 2021. På föredragning av statsrådet beviljade republikens president den 19 november 2021 fullmakt att underteckna överenskommelsen. Överenskommelsen undertecknades i Haag den 22 februari 2022.

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 förpliktelser som gäller informationssäkerhet uppfylls. Utrikesministeriet är Finlands nationella säkerhetsmyndighet (National Security Authority, NSA) i uppfyllandet av internationella förpliktelser som gäller informationssäkerhet. Försvarsministeriet, huvudstaben, skyddspolisen och 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 *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 integritetsskyddet 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 eller 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 uppräkningslista 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 Nederländerna och som Nederländerna lämnar ut till Finland skyddas och hanteras korrekt. Överenskommelsen syftar också till att främja parternas möjligheter att ta emot säkerhetsklassificerad information från varandra och så förbättra samarbetet mellan länderna inom informationssäkerhetsområdet. Ytterligare syftar överenskommelsen till att trygga parternas företags möjligheter att delta i sådana internationella projekt eller projekt mellan Finland och Nederländerna som kan kräva utbyte av säkerhetsklassificerad information.

4 De viktigaste förslagen

I denna proposition föreslås det att riksdagen godkänner överenskommelsen mellan Finland och Nederländerna om utbyte och ömsesidigt skydd av säkerhetsklassificerad information. Propositionen innehåller också ett förslag till en 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 Nederländerna

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 Nederländerna gäller handlingar som Nederländerna 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 Nederländerna 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 Nederländerna 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 Nederländerna. Analogt öppnar överenskommelsen möjligheter för nederländska 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 nederländska 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 informations-säkerhet.

I enlighet med överenskommelsens artikel 6.3 om säkerhetssamarbete ska säkerhetsmyndigheterna på begäran bistå varandra vid förfarandena för säkerhetsutredningar i enlighet med nationella lagar och bestämmelser.

6 Remissvar

Utkastet till proposition var på remiss på webbplatsen utlåtande.fi mellan den 25.1.2023 och den 28.2.2023. Propositionen sändes på remiss till justitieministeriet, arbets- och näringsministeriet, försvarsministeriet, finansministeriet, inrikesministeriet, kommunikationsministeriet, Skyddspolisens, Huvudstaben samt Transport- och kommunikationsverket. Dessutom har även andra än de som nämns ovan i sändlistan kunnat lämna utlåtande. Inga utlåtande gavs.

7 Bestämmelserna i överenskommelsen och deras förhållande till lagstiftningen i Finland

Artikel 1. Syfte. I artikeln definieras att syftet med överenskommelsen är att säkerställa skyddet av säkerhetsklassificerad information som utbyts mellan parterna eller juridiska eller fysiska personer inom deras jurisdiktion eller som skapas inom ramen för ett bilateralt program enligt överenskommelsen. 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:

Enligt punkt a avses med säkerhetsklassificerat kontrakt ett kontrakt eller underleverantörskontrakt som förutsätter eller som har anknytning till säkerhetsklassificerad information. Denna punkt är i samklang med 2 § 3 mom. i lagen om internationella förpliktelser som gäller informations-säkerhet.

I punkt b definieras säkerhetsklassificerad information. Överenskommelsen gäller all information och material som har säkerhetsklassificerats av någondera parten och vars obehöriga röjande eller förlust i olika grad skulle kunna skada någondera partens eller båda parternas intressen. Denna punkt är i samklang med definitionen av särskilt känsligt informationsmaterial i 2 § 1 mom. 2 punkten i lagen om internationella förpliktelser som gäller informations-säkerhet.

Enligt punkt c avses med behörig säkerhetsmyndighet en nationell säkerhetsmyndighet eller något annat behörigt organ som i enlighet med parternas nationella lagar och bestämmelser har bemyndigats att svara för genomförandet och efterlevnaden av överenskommelsen.

Enligt punkt d avses med kontraktspart en fysisk eller juridisk person som har rättskapacitet att ingå kontrakt.

Enligt punkt e avses med säkerhetsutredning av företag en positiv bedömning av den behöriga säkerhetsmyndigheten om att ett företag har vidtagit lämpliga säkerhetsåtgärder och kan beviljas tillgång till samt hantering av säkerhetsklassificerad information upp till och inklusive en angiven nivå i enlighet med nationella lagar och bestämmelser.

Enligt punkt f avses med informationsbehov en fysisk eller juridisk persons behov av att få tillgång till, få kännedom om eller komma i besittning av säkerhetsklassificerad information för att utföra officiella uppgifter eller tjänster.

Enligt punkt g avses med ursprungspart den part under vars överinseende den säkerhetsklassificerade informationen har skapats.

Enligt punkt h avses med säkerhetsutredning av person en positiv bedömning av den behöriga säkerhetsmyndigheten om att en fysisk person har genomgått en säkerhetsutredning och kan beviljas tillgång till samt hantering av säkerhetsklassificerad information upp till och inklusive en angiven nivå i enlighet med nationella lagar och bestämmelser.

Enligt punkt i avses med utlämnande part den part eller den kontraktspart inom partens jurisdiktion som lämnar ut säkerhetsklassificerad information till den mottagande parten i enlighet med denna överenskommelse.

Enligt punkt j avses med mottagande part den part eller den kontraktspart inom partens jurisdiktion som tar emot säkerhetsklassificerad information av den utlämnande parten i enlighet med denna överenskommelse.

Enligt punkt k avses med säkerhetsklassificeringsanvisningar en handling som hänför sig till ett säkerhetsklassificerat kontrakt och där de delar i kontraktet som innehåller säkerhetsklassificerad information fastställs och de tillämpliga säkerhetsklasserna anges.

Enligt punkt l avses med informationssäkerhetsincident en gärning eller försummelse i strid med nationella lagar och bestämmelser som leder till obehörig tillgång till eller röjande, förlust eller äventyrande av den andra partens säkerhetsklassificerade information.

Enligt punkt m avses med tredje part en sådan internationell organisation eller stat, inklusive juridiska eller fysiska personer inom dess jurisdiktion, som inte är part i denna överenskommelse.

Artikel 3. Behöriga säkerhetsmyndigheter Enligt artikel 1.1 anges parternas behöriga myndigheter i bilaga 1 till 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 Nederländerna har National Security Authority (NSA), General Intelligence and Security Service samt Ministry of Interior and Kingdom Relations utsetts till behöriga säkerhetsmyndigheter.

Enligt punkt 2 ska de behöriga säkerhetsmyndigheterna ge varandra officiella kontaktuppgifter.

Artikel 4. Säkerhetsklasser. I punkt 1 definieras hur Finlands och Nederländernas säkerhetsklasser motsvarar varandra. Den högsta säkerhetsklassen, som kräver de strängaste informat-

ionssäkerhetsåtgärderna, är "ERITTÄIN SALAINEN / YTTERST HEMLIG" (Stg ZEER GEHEIM, TOP SECRET). Till denna kategori räknas i Finland information som, om den obehörigen 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" (Stg GEHEIM, SECRET). 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" (Stg CONFIDENTIEEL, CONFIDENTIAL). 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 TILGÅNG" (DEPARTEMENTAAL VERTROUWELIJK, RESTRICTED) 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 t.ex. vara skyddet av säkerhetsarrangemangen för statsledningen och statsbesök och för datasystem (24 § 1 mom. 7 punkten) samt samhällsekonomin (24 § 1 mom. 11 och 12 punkten). Allmänt tillämpliga bestämmelser om sekretess- och klassificeringsanteckningar i myndighetshandlingar ingår i 25 § i offentlighetslagen. Enligt 25 § 3 mom. 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 besvärssärenden säkerhetsklassificera handlingar och förse dem med anteckning om säkerhetsklass som visar vilket slag av informationsssäkerhetsåtgärder 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 förse 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 förse 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 förse med en sådan märkning 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 2 ska parterna vidta alla lämpliga åtgärder för att säkerställa att den mottagande parten förser all sådan säkerhetsklassificerad information som avses i överenskommelsen och som den har tagit emot från den utlämnande parten med en anteckning som anger informationens säkerhetsklass och som motsvarar den säkerhetsklass som ursprungsparten har gett den i enlighet med punkt 1.

Enligt punkt 3 ska parterna vidta alla lämpliga åtgärder för att säkerställa att den mottagande parten inte utan skriftligt samtycke av ursprungsparten ändrar eller upphäver säkerhetsklassificeringen av sådan säkerhetsklassificerad information som avses i överenskommelsen.

Enligt punkt 4 ska ursprungsparten säkerställa att den mottagande parten underrättas om eventuella ändringar av säkerhetsklassen för den säkerhetsklassificerade information som har lämnats ut.

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. Vid elektronisk förmedling av säkerhetsklassificerad information i ett oskyddat nätverk ska den mottagande parten använda krypteringsverktyg.

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

Enligt punkt 3 ska tillgång till säkerhetsklassificerad information beviljas endast sådana fysiska personer som har ett informationsbehov, som har instruerats om sitt ansvar i skyddet av säkerhetsklassificerad information, som har undertecknat en sekretessförbindelse och/eller som har en lagstadgad tystnadsplikt för vilka respektive säkerhetsklass motsvarande intyg över säkerhetsutredning av person har utfärdats eller som på grund av sina uppgifter på behörigt sätt fått tillgång till säkerhetsklassificerad information, i samtliga fall i enlighet med gällande nationella lagar och bestämmelser.

Enligt punkt 4 krävs inte säkerhetsutredning av person för tillgång till säkerhetsklassificerad information i en säkerhetsklass som motsvarar den i artikel 4 i denna överenskommelse nämnda säkerhetsklassen "RESTRICTED".

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

Enligt 1 punkt ska de behöriga säkerhetsmyndigheterna, för att säkerställa att parternas säkerhetskrav motsvarar varandra, på begäran informera varandra om sina nationella lagar, bestämmelser, verksamhetsprinciper och rutiner för skydd av säkerhetsklassificerad information.

Enligt punkt 2 ska den ena partens behöriga säkerhetsmyndighet, på begäran av den andra partens behöriga säkerhetsmyndighet, skriftligen bekräfta att ett giltigt intyg om säkerhetsutredning av person eller av företag har utfärdats.

Enligt punkt 3 ska de behöriga säkerhetsmyndigheterna, i enlighet med parternas gällande nationella lagar och bestämmelser, på begäran bistå varandra vid utförandet av säkerhetsutredningar av företag eller av person.

Enligt punkt 4 ska de behöriga säkerhetsmyndigheterna utan dröjsmål skriftligen underrätta varandra om ändringar i bekräftat utfärdade intyg över vedertagna säkerhetsutredningar av person eller av företag.

Enligt punkt 5 ska samarbetet inom ramen för denna överenskommelse ska ske på engelska.

Artikel 7. Säkerhetsklassificerade kontrakt. Artikeln innehåller bestämmelser om ingående av sådana säkerhetsklassificerade kontrakt inom någondera partens territorium som avses i artikel 2 punkt a.

Enligt punkt 1 ska den mottagande partens behöriga säkerhetsmyndighet på begäran meddela ursprungspartens behöriga säkerhetsmyndighet huruvida ett sådant lämpligt intyg över säkerhetsutredning av företag som motsvarar den säkerhetsklass som krävs har utfärdats till den föreslagna kontraktsparten, som deltar i förhandlingar som föregår säkerhetsklassificerade kontrakt.

Om en part eller en kontraktspart som omfattas av partens jurisdiktion ingår ett säkerhetsklassificerat kontrakt i en säkerhetsklass som motsvarar den i artikel 4 i denna överenskommelse nämnda säkerhetsklassen "CONFIDENTIAL" eller en högre klass med en kontraktspart eller underleverantör som omfattas av den andra partens jurisdiktion ska den förstnämnda parten eller kontraktsparten enligt punkt 2 få en skriftlig bekräftelse från den andra parten om att den andra partens kontraktspart har fått ett intyg över säkerhetsutredning av företag.

Enligt 3 punkten får den mottagande partens behöriga säkerhetsmyndighet vid öppna anbuds-förfaranden utan formell begäran överlämna de relevanta intygen över säkerhetsutredning av företag till ursprungspartens behöriga säkerhetsmyndighet.

Enligt punkt 4 krävs inte säkerhetsutredning av företag för tillgång till säkerhetsklassificerade kontrakt i en säkerhetsklass som motsvarar den i artikel 4 i denna överenskommelse nämnda säkerhetsklassen "RESTRICTED".

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.

Enligt 6 punkten ska samtliga säkerhetsklassificerade kontrakt som ingås i enlighet med denna överenskommelse innehålla säkerhetskrav som tar hänsyn till följande:

- a) säkerhetsklassificeringsanvisningar,
- b) kontaktuppgifter till de behöriga säkerhetsmyndigheter som ansvarar för genomförandet av säkerhetsklassificerade kontrakt och för tillsynen över skyddet av säkerhetsklassificerad information med anknytning till överenskommelsen,
- c) lagar och bestämmelser som gäller skydd av säkerhetsklassificerad information,
- d) förfarandet och kraven för tillgång till säkerhetsklassificerad information,
- e) hantering och lagring av säkerhetsklassificerad information,
- f) överföring och elektronisk förmedling av säkerhetsklassificerad information,
- g) märkning av säkerhetsklassificerad information,
- h) skyldighet att övervaka säkerhetsbeteenden och underrätta den nationella behöriga säkerhetsmyndigheten om eventuella informationssäkerhetsincidenter,
- i) skyddet av säkerhetsklassificerad information efter det att ett kontrakt har löpt ut,
- j) utplåning eller återlämnande av säkerhetsklassificerad information,
- k) utlämnande av uppgifter om ett säkerhetsklassificerat kontrakt.

Enligt 7 punkten ska den behöriga säkerhetsmyndigheten för den part som godkänner ingåendet av ett säkerhetsklassificerat kontrakt sända en kopia av den del av kontraktet som gäller säkerhetskraven till den mottagande partens behöriga säkerhetsmyndighet för att underlätta tillsynen över säkerhetsaspekter i fråga om kontraktet.

Enligt 8 punkten ska godkännande av besök ske i enlighet med de förfaranden som anges i artikel 10 i denna överenskommelse, när verksamhet som bygger på ett säkerhetsklassificerat kontrakt är förenad med besök av någondera partens personal i den andra partens land.

Enligt 9 punkten ska kontraktsparter och underleverantörer säkerställa att denna artikel iakttas, om en kontraktspart låter en underleverantör genomföra delar av ett säkerhetsklassificerat kontrakt.

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

Enligt 1 punkten förmedlas säkerhetsklassificerad information i enlighet med den utlämnande partens nationella lagar och bestämmelser eller på något annat sätt som avtalas mellan de behöriga säkerhetsmyndigheterna.

Enligt 2 punkten får parterna i enlighet med de förfaranden som godkänts av de behöriga säkerhetsmyndigheterna elektroniskt förmedla säkerhetsklassificerad information som skyddas med krypteringssätt .

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 9. Kopiering, översättning, och utplåning av säkerhetsklassificerad information. Enligt 1 punkten ska kopior och översättningar av säkerhetsklassificerad information förses med märkning och skyddas på samma sätt som den ursprungliga säkerhetsklassificerade informationen.

Enligt 2 punkten ska antalet översättningar och kopior begränsas till det minimum användning enligt överenskommelsen kräver och de får endast göras av personer som enligt nationella lagar och bestämmelser har rätt att få tillgång till säkerhetsklassificerad information i samma säkerhetsklass som den säkerhetsklassificerade information som översätts eller kopieras.

Enligt punkt 3 ska översättningar förses med en tillämplig märkning på översättningens språk om att de innehåller säkerhetsklassificerad information från den utlämnande parten.

Säkerhetsklassificerad information i en säkerhetsklass som motsvarar den i artikel 4 i denna överenskommelse nämnda säkerhetsklassen ”TOP SECRET” får enligt punkt 4 inte översättas eller kopieras utan ursprungspartens skriftliga förhandssamtycke.

Säkerhetsklassificerad information i en säkerhetsklass som motsvarar den i artikel 4 i denna överenskommelse nämnda säkerhetsklassen ”TOP SECRET” får enligt punkt 5 inte utplånas utan ursprungspartens skriftliga förhandssamtycke. Informationen ska återlämnas till ursprungsparten efter det att den utlämnande parten och den mottagande parten anser att informationen inte längre behövs.

Enligt 6 punkten ska säkerhetsklassificerad information upp till och inklusive den i artikel 4 i denna överenskommelse nämnda säkerhetsklassen ”SECRET” utplånas i enlighet med nationella lagar och bestämmelser när den mottagande parten anser att informationen inte längre behövs.

Enligt punkt 7 ska informationen, om en krissituation gör det omöjligt att skydda säkerhetsklassificerad information som har lämnats ut i enlighet med denna överenskommelse, omedelbart utplånas. Den mottagande parten ska utan dröjsmål skriftligen 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 10. Besök. Enligt 1 punkten krävs skriftligt förhandssamtycke av den berörda behöriga säkerhetsmyndigheten för besök som förutsätter tillgång till säkerhetsklassificerad information i och högre än den i artikel 4 i denna överenskommelse nämnda säkerhetsklass "CONFIDENTIAL", om inte de behöriga säkerhetsmyndigheterna sinsemellan avtalar om något annat.

Enligt 2 punkten ska besökare minst fjorton dagar före den föreslagna tidpunkten för besöket lämna en begäran om besök till den behöriga säkerhetsmyndigheten, som förmedlar begäran till den andra partens behöriga säkerhetsmyndighet. I brådskande fall kan en begäran om besök lämnas inom en kortare tidsfrist, om de behöriga säkerhetsmyndigheterna kommer överens om detta på förhand.

Enligt 3 punkten ska begäran om besök ska innehålla följande uppgifter:

- a) besökarens hela namn, födelsedatum och födelseort, medborgarskap samt passets eller identitetskortets nummer,
- b) besökarens officiella befattning och namnet på den organisation som han eller hon företräder,
- c) bekräftelse av intyg över säkerhetsutredning av person som har utfärdats besökaren samt intygets giltighet,
- d) besökets tidpunkt och längd. För upprepade besök ska hela den period under vilken besöken kommer att äga rum anges,
- e) besökets syfte och säkerhetsklassen för den säkerhetsklassificerade information som sannolikt diskuteras med besökaren eller som han eller hon antas få tillgång till,
- f) namn på och adress, telefonnummer, faxnummer och e-postadress till samt kontaktperson vid den anläggning som ska besökas,
- g) daterad och stämplad underskrift av en företrädare för den behöriga säkerhetsmyndigheten i besökarens land.

Enligt punkt 4 kan de behöriga säkerhetsmyndigheterna sinsemellan komma överens om en förteckning över besökare som är berättigade till upprepade besök. De behöriga säkerhetsmyndigheterna ska sinsemellan komma överens om övriga detaljer i fråga om upprepade besök. Tillstånd för upprepade besök är dock giltiga i högst 12 månader.

Enligt 5 punkten behandlas sådan säkerhetsklassificerad information som har lämnats till eller förvärvat av en besökare i enlighet med bestämmelserna i denna överenskommelse.

Artikel 11. Informationssäkerhetsincident. Enligt punkt 1 ska de behöriga säkerhetsmyndigheterna omedelbart skriftligen underrätta varandra om upptäckta eller misstänkta informationssäkerhetsincidenter som inkluderar säkerhetsklassificerad information.

Enligt punkt 2 ska den mottagande parten omedelbart utreda den upptäckta eller misstänkta informationssäkerhetsincidenten. Ursprungspartens behöriga säkerhetsmyndighet ska vid behov samarbeta vid utredningen.

Enligt punkt 3 ska den behöriga säkerhetsmyndigheten, i enlighet med sina nationella lagar och bestämmelser, vidta lämpliga åtgärder för att begränsa följderna av en informationssäkerhetsincident och förhindra att den upprepas. Ursprungspartens behöriga säkerhetsmyndighet ska underrättas om resultatet av utredningen och om eventuella åtgärder som har vidtagits.

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 stå för sina kostnader när de uppfyller förpliktelserna enligt denna överenskommelse.

Artikel 13. Tvistlösning. Enligt artikeln ska tvister om tolkningen och tillämpningen av denna överenskommelse uteslutande lösas genom samråd mellan parterna.

Artikel 14. Förhållande till andra överenskommelser. Enligt artikeln ersätter denna överenskommelse inte sådana internationella överenskommelser som redan har ingåtts eller som kan komma att ingås och som uttryckligen avser rättshandlingar som annars skulle omfattas av överenskommelsen.

Artikel 15. Genomförandearrangemang. Enligt artikeln får parternas behöriga säkerhetsmyndigheter vidta genomförandearrangemang i enlighet med överenskommelsen.

Artikel 16. Slutbestämmelser. Artikeln innehåller bestämmelser om ikraftträdande, geografisk tillämpning, 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 gäller överenskommelsen 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 månader. Om överenskommelsen sägs upp med stöd av artikeln i fråga ska information som redan har lämnats ut eller skapats inom ramen för överenskommelsen skyddas i enlighet med överenskommelsen så länge informationen är säkerhetsklassificerad.

8 Specialmotivering till lagförslaget

I 95 § i Finlands grundlag förutsätts det att de bestämmelser i internationella förpliktelser som hör till området för lagstiftningen sätts i kraft nationellt genom en särskild ikraftträdandelag. Sådana bestämmelser ska sättas i kraft genom en lag också när det till följd av förpliktelsen inte är nödvändigt att justera det materiella innehållet i den nationella lagstiftningen. Eftersom det inte är nödvändigt att ändra den materiella lagstiftningen för att genomföra förpliktelserna i överenskommelsen om informationssäkerhet mellan Finland och Nederländerna, innehåller propositionen endast ett förslag till en blankettlag.

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

2 §. Om sättande i kraft av de bestämmelser i avtalet som inte hör till området för lagstiftningen och om ikraftträdandet av lagen bestäms genom förordning av statsrådet. Avsikten är att lagen ska träda i kraft samtidigt som avtalet träder i kraft för Finlands del.

9 Ikraftträdande

Enligt artikel 16.1 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 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 ändringsfördraget träder i kraft, vid en tidpunkt som fastställs genom förordning av statsrådet.

10 Bifall av Ålands lagting

Enligt 59 § 1 mom. i självstyrelselagen för Åland (1144/1991) träder en bestämmelse i ett fördrag eller någon annan internationell förpliktelse som Finland ingår eller förbinder sig till och som innehåller en bestämmelse i en fråga som enligt självstyrelselagen för Åland faller inom landskapets behörighet i kraft i landskapet endast om lagtinget ger sitt bifall till den författning genom vilken bestämmelsen sätts i kraft.

De 25 överenskommelser om informationssäkerhet som är i kraft i Finland har inte ansetts innehålla bestämmelser som skulle falla inom landskapets behörighet och således har lagtingets bifall inte begärts för ikraftträdandeförfattningarna.

Enligt regeringen innehåller överenskommelsen med Nederländerna om utbyte och ömsesidigt skydd av säkerhetsklassificerad information inte heller några bestämmelser som faller inom landskapet Ålands behörighet och förutsätter således inte landskapets bifall i enlighet med 59 § i självstyrelselagen för Åland. Landskapsregeringens ståndpunkt om behörighetsfördelningen gällande informationssäkerhetsavtal beskrivs i regeringens proposition RP 4/2023 rd, ss 23 och 24.

Grundlagsutskottet har påpekat vid behandling av regeringens proposition om RP 315/2022 rd om nordatlantiska fördraget att det utifrån tidigare praxis för godkännande av internationella avtal är möjligt att i en senare fas begära lagtingets bifall för godkännande av internationella avtal, om det visar sig nödvändigt (GrUU 80/2022 rd, s. 10).

11 Behovet av riksdagens samtycke samt behandlingsordning

11.1 Behovet av riksdagens samtycke

Enligt 94 § 1 mom. i grundlagen krävs riksdagens godkännande för fördrag och andra internationella förpliktelser som innehåller sådana bestämmelser som hör till området för lagstiftningen.

Enligt grundlagsutskottets tolkningspraxis ska en bestämmelse anses höra till området för lagstiftningen om den gäller utövande eller begränsning av någon grundläggande fri- eller rättighet som är skyddad i grundlagen, om den i övrigt gäller grunderna för individens rättigheter och skyldigheter, om den sak som bestämmelsen gäller är sådan att om den enligt grundlagen ska föreskrivas i lag eller om det finns lagbestämmelser om den sak som bestämmelsen gäller eller om det enligt rådande uppfattning i Finland ska lagstiftas om saken. 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).

Enligt artikel 3 i överenskommelsen anges de behöriga säkerhetsmyndigheterna i bilaga I till överenskommelsen. I bilagan 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 informations säkerhet. 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 informations säkerhet 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 informations säkerhet 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 informations säkerhet ska särskilt känsligt informationsmaterial trots offentlighetslagens bestämmelser sekretessbeläggas, om inte annat följer av en internationell förpliktelse som gäller informations säkerhet. 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 tryggt 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 bestämmelse som motsvarar denna förpliktelse 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 7 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. Således hör bestämmelserna i artikeln till området för lagstiftningen.

11.2 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 förpliktelserna 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 Nederländerna 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 Haag den 22 februari 2022 mellan Republiken Finland och Konungariket Nederländerna ingångna överenskommelsen om utbyte och ömsesidigt skydd av säkerhetsklassificerad information.

Kläm 2

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

Lag

om överenskommelsen med Nederländerna om utbyte och ömsesidigt skydd av säkerhetsklassificerad information

I enlighet med riksdagens beslut föreskrivs:

1 §

De bestämmelser som hör till området för lagstiftningen i den i Haag den 22 februari 2022 mellan Republiken Finland och Konungariket Nederländerna ingångna överenskommelsen om utbyte och 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 5 Oktober 2023

Statsminister

Petteri Orpo

Utrikesminister Elina Valtonen

**ÖVERENSKOMMELSE
MELLAN REPUBLIKEN FINLAND
OCH
KONUNGARIKET NEDERLÄNDERNA
OM UTBYTE OCH ÖMSESIDIGT
SKYDD AV SÄKERHETSKLASSIFICE-
RAD INFORMATION**

Republiken Finland och Konungariket Nederländerna, nedan ”parterna”,

har för att säkerställa det ömsesidiga skyddet av säkerhetsklassificerad information med hänsyn till den nationella säkerheten kommit överens om följande:

Artikel 1
Syfte

Syftet med denna överenskommelse är att säkerställa skyddet av sådan säkerhetsklassificerad information som utbyts mellan parterna eller mellan juridiska eller fysiska personer inom deras jurisdiktion, eller som skapas inom ramen för ett bilateralt program enligt denna överenskommelse. Denna överenskommelse innehåller bestämmelser om säkerhetsförfaranden och arrangemang för detta skydd.

Artikel 2
Definitioner

I denna överenskommelse avses med
a) ”**säkerhetsklassificerat kontrakt**” ett kontrakt eller underleverantörskontrakt som förutsätter eller som har anknytning till säkerhetsklassificerad information,

**AGREEMENT
BETWEEN THE REPUBLIC OF
FINLAND
AND
THE KINGDOM OF THE
NETHERLANDS
CONCERNING THE EXCHANGE AND
MUTUAL PROTECTION OF CLASSI-
FIED INFORMATION**

The Republic of Finland and the Kingdom of the Netherlands, Hereinafter referred to as “the Parties”,

In order to ensure the mutual protection of Classified Information have, in the interests of national security, agreed upon the following:

Article 1
Purpose

The purpose of this Agreement is to ensure the protection of Classified Information exchanged between the Parties or between legal entities or individuals under their jurisdiction, or generated in the framework of a bilateral program under this Agreement. The Agreement sets out the security procedures and arrangements for such protection.

Article 2
Definitions

For the purpose of this Agreement:
a) “**Classified Contract**” means any contract or subcontract, which requires or involves Classified Information.

b) ”**säkerhetsklassificerad information**” information eller material som har säkerhetsklassificerats av någondera parten och vars obehöriga röjande eller förlust i olika grad skulle kunna skada någondera partens eller båda parternas intressen,

c) ”**behörig säkerhetsmyndighet**” nationell säkerhetsmyndighet eller något annat behörigt organ som i enlighet med parternas nationella lagar och bestämmelser har bemyndigats att svara för genomförandet och efterlevnaden av denna överenskommelse,

d) ”**kontraktspart**” fysisk eller juridisk person som har rättskapacitet att ingå kontrakt,

e) ”**säkerhetsutredning av företag**” en positiv bedömning av den behöriga säkerhetsmyndigheten om att ett företag har vidtagit lämpliga säkerhetsåtgärder och kan beviljas tillgång till samt hantering av säkerhetsklassificerad information upp till och inklusive en angiven nivå i enlighet med nationella lagar och bestämmelser,

f) ”**informationsbehov**” en fysisk eller juridisk persons behov av att få tillgång till, få kännedom om eller komma i besittning av säkerhetsklassificerad information för att utföra officiella uppgifter eller tjänster,

g) ”**ursprungspart**” den part under vars överinseende den säkerhetsklassificerade informationen har skapats,

e) ”**säkerhetsutredning av person**” en positiv bedömning av den behöriga säkerhetsmyndigheten om att en fysisk person har genomgått en säkerhetsutredning och kan beviljas tillgång till samt hantering av säkerhetsklassificerad information upp till och inklusive en angiven nivå i enlighet med nationella lagar och bestämmelser,

i) ”**utlämnande part**” den part eller den kontraktspart inom partens jurisdiktion som lämnar ut säkerhetsklassificerad information till den mottagande parten i enlighet med denna överenskommelse,

b) ”**Classified Information**” means any information or material designated by a security classification by one of the Parties the unauthorised disclosure or loss of which could cause varying degrees of prejudice to the interests of one or both of the Parties.

c) ”**Competent Security Authority**” means a National Security Authority or any other competent body authorised in accordance with the national laws and regulations of the Parties which is responsible for the implementation of and compliance with this Agreement.

d) ”**Contractor**” means any individual or legal entity with the capacity to enter into contracts.

e) ”**Facility Security Clearance**” means the positive determination by the Competent Security Authority that a facility has in place appropriate security measures to access and handle Classified Information up to and including a specified security classification level, in accordance with national laws and regulations.

f) ”**Need to know**” means the requirement for an individual or a legal entity for access to, knowledge of or possession of Classified Information to perform official tasks or services.

g) ”**Originating Party**” means the Party under whose authority Classified Information has been created.

h) ”**Personnel Security Clearance**” means the positive determination by the Competent Security Authority that an individual has been security cleared to access and handle Classified Information up to and including a specified classification level, in accordance with its national laws and regulations.

j) ”**mottagande part**” den part eller den kontraktspart inom partens jurisdiktion som tar emot säkerhetsklassificerad information av den utlämnande parten i enlighet med denna överenskommelse,

k) ”**säkerhetsklassificeringsanvisningar**” en handling som hänför sig till ett säkerhetsklassificerat kontrakt och där de delar i kontraktet som innehåller säkerhetsklassificerad information fastställs och de tillämpliga säkerhetsklasserna anges,

l) ”**informationssäkerhetsincident**” en gärning eller försummelse i strid med nationella lagar och bestämmelser som leder till obehörig tillgång till eller röjande, förlust eller äventyrande av den andra partens säkerhetsklassificerade information,

m) ”**tredje part**” en sådan internationell organisation eller stat, inklusive sådana juridiska och fysiska personer inom dess jurisdiktion som inte är part i denna överenskommelse.

Artikel 3

Behöriga säkerhetsmyndigheter

1. Parternas behöriga säkerhetsmyndigheter anges i bilaga 1 till denna överenskommelse.

2. De behöriga säkerhetsmyndigheterna ska ge varandra officiella kontaktuppgifter.

Artikel 4

Säkerhetsklasser

1. Följande säkerhetsklasser hos parterna motsvarar varandra och de säkerhetsklasser som fastställs i parternas nationella lagstiftning:

i) ”**Providing Party**” means the Party or Contractor under its jurisdiction, which provides Classified Information to the Receiving Party under this Agreement.

j) ”**Receiving Party**” means the Party or Contractor under its jurisdiction, which receives Classified Information from the Providing Party under this Agreement.

k) ”**Security Classification Guide**” means a document associated with a Classified Contract that identifies each part of that Classified Contract which contains Classified Information, specifying the applicable security classification levels.

l) ”**Security Incident**” means an act or an omission, contrary to national laws and regulations, which results in unauthorised access, disclosure, loss or compromise of Classified Information of the other Party.

m) ”**Third Party**” means any international organisation or state, including legal entities or individuals under its jurisdiction, which is not a Party to this Agreement.

Article 3

Competent Security Authorities

1. The Competent Security Authorities of the Parties are listed in Annex 1 of this Agreement.

2. The Competent Security Authorities shall provide each other with official contact details.

Article 4

Security classification levels

1. The following security classifications of the Parties are equivalent and correspond to the security classification levels specified in their national legislation:

| I Republiken Finland For the Republic of Finland | I Konungariket Nederländerna, For the Kingdom of the Netherlands | Motsvarighet på engelska Equivalent in English¹ |
|---|---|---|
| ERITTÄIN SALAINEN eller / or YTTERST HEMLIG | Stg ZEER GEHEIM | TOP SECRET |
| SALAINEN eller / or HEMLIG | Stg GEHEIM | SECRET |
| LUOTTAMUKSELLINEN eller / or KONFIDENTIELL | Stg CONFIDENTIEEL | CONFIDENTIAL |
| KÄYTTÖ RAJOITETTU eller / or BEGRÄNSAD TILLGÅNG | DEPARTEMENTAAL VERTROUWELIJK | RESTRICTED |

2. Parterna ska vidta alla lämpliga åtgärder för att säkerställa att den mottagande parten förser all sådan säkerhetsklassificerad information som avses i denna överenskommelse och som den tagit emot av den utlämnande parten med en märkning om säkerhetsklass som motsvarar den säkerhetsklass som ursprungsparten har angett i enlighet med det syfte som anges i artikel 1 i denna överenskommelse.

3. Parterna ska vidta alla lämpliga åtgärder för att säkerställa att den mottagande parten inte utan skriftligt samtycke av ursprungsparten ändrar eller upphäver säkerhetsklassificeringen av sådan säkerhetsklassificerad information som den tar emot och som avses i denna överenskommelse.

2. The Parties shall take all appropriate measures to ensure that the Receiving Party shall mark all the Classified Information under this Agreement that it has received from the Providing Party with the security classification that corresponds to the security classification given by the Originating Party in accordance with the scheme contained in paragraph 1 of this Article.

3. The Parties shall take all appropriate measures to ensure that the Receiving Party shall not modify or revoke the security classification of received Classified Information under this Agreement without the written approval of the Originating Party.

¹När denna överenskommelse tillämpas ska den engelska motsvarigheten i denna säkerhetsklass användas. De officiella säkerhetsklasser som används för märkning av säkerhetsklassificerad information anges på finska/svenska och nederländska.

4. Ursprungsparten ska säkerställa att den mottagande parten underrättas om eventuella ändringar av säkerhetsklassen för den säkerhetsklassificerade information som har lämnats ut.

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. Vid elektronisk förmedling av säkerhetsklassificerad information i ett oskyddat nätverk ska den mottagande parten använda krypteringsverktyg.

2. Parterna ska inte ge tredje parter tillgång till säkerhetsklassificerad information utan ursprungspartens skriftliga förhandssamtycke.

3. Tillgång till säkerhetsklassificerad information beviljas endast sådana fysiska personer som har ett informationsbehov, som har instruerats om sitt ansvar i skyddet av säkerhetsklassificerad information, som har undertecknat en sekretessförbindelse och/eller som har en lagstadgad tystnadsplikt och för vilka respektive säkerhetsklass motsvarande intyg över säkerhetsutredning av person har utfärdats eller som på grund av sina uppgifter på behörigt sätt fått tillgång till säkerhetsklassificerad information, i samtliga fall i enlighet med gällande nationella lagar och bestämmelser.

4. Säkerhetsutredning av person krävs inte för tillgång till säkerhetsklassificerad information i en säkerhetsklass som motsvarar den i artikel 4 i denna överenskommelse nämnda säkerhetsklassen "RESTRICTED".

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

4. The Originating Party shall ensure that the Receiving Party will be informed of any change in the security classification level of the Classified Information provided.

Article 5

Protection of Classified Information

1. The Parties shall take all appropriate measures in accordance with their national laws and regulations so as 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. Electronic transmission of Classified Information in an unprotected network by the Receiving Party shall take place using cryptographic tools.

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', are briefed on their responsibilities for the protection of Classified Information, have signed a statement of confidentiality and/or are legally bound to confidentiality and who hold a Personnel Security Clearance at the corresponding level or are authorised to have access to such information by virtue of their function, all in accordance with national laws and regulations.

4. A Personnel Security Clearance is not required for access to Classified Information at the security classification level equivalent to "RESTRICTED" as mentioned in Article 4 of this Agreement.

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

Artikel 6
Säkerhetssamarbete

1. För säkerställande av att parternas säkerhetskrav motsvarar varandra ska de behöriga säkerhetsmyndigheterna på begäran informera varandra om sina nationella lagar, bestämmelser, verksamhetsprinciper och rutiner för skydd av säkerhetsklassificerad information.

2. På begäran av den ena partens behöriga säkerhetsmyndighet ska den andra partens behöriga säkerhetsmyndighet skriftligen bekräfta att ett giltigt intyg över säkerhetsutredning av person eller av företag har utfärdats.

3. I enlighet med parternas gällande nationella lagar och bestämmelser ska de behöriga säkerhetsmyndigheterna på begäran bistå varandra vid utförandet av säkerhetsutredning av företag eller av person.

4. De behöriga säkerhetsmyndigheterna ska utan dröjsmål skriftligen underrätta varandra om ändringar i bekräftat utfärdade intyg över vedertagna säkerhetsutredningar av person eller av företag.

5. Samarbetet inom ramen för denna överenskommelse ska ske på engelska.

Artikel 7
Säkerhetsklassificerade kontrakt

1. Den mottagande partens behöriga säkerhetsmyndighet ska på begäran meddela ursprungspartens behöriga säkerhetsmyndighet huruvida ett sådant lämpligt intyg över säkerhetsutredning av företag som motsvarar den säkerhetsklass som krävs har utfärdats till den föreslagna kontraktsparten, som deltar i förhandlingar som föregår säkerhetsklassificerade kontrakt.

Article 6
Security co-operation

1. In order to maintain comparable standards of security, the Competent Security Authorities shall, on request, inform each other about their national laws and regulations, policies and practices for protecting Classified Information.

2. On request of the Competent Security Authority of one Party, the Competent Security Authority of the other Party shall issue a written confirmation that a valid Personnel Security Clearance or Facility Security Clearance has been issued.

3. The Competent Security Authorities shall assist each other in carrying out Facility Security Clearance and Personnel Security Clearance investigations on request and in accordance with national laws and regulations.

4. The Competent Security Authorities shall promptly notify each other in writing about changes in recognised Personnel Security Clearances and Facility Security Clearances for whom or for which a confirmation has been provided.

5. The co-operation under this Agreement shall be effected in English.

Article 7
Classified Contracts

1. Upon request, the Competent Security Authority of the Receiving Party shall inform the Competent Security Authority of the Originating Party whether a proposed Contractor participating in precontract negotiations of a Classified Contract has been issued an appropriate Facility Security Clearance corresponding to the required security classification level.

2. If a Party or a Contractor under its jurisdiction grants a Classified Contract at the Security Classification Levels equivalent to "CONFIDENTIAL" or above as mentioned

2. Om en part eller en kontraktspart som omfattas av partens jurisdiktion ingår ett säkerhetsklassificerat kontrakt i en säkerhetsklass som motsvarar den i artikel 4 i denna överenskommelse nämnda säkerhetsklassen "CONFIDENTIAL" eller en högre klass med en kontraktspart eller underleverantör som omfattas av den andra partens jurisdiktion ska den förstnämnda parten eller kontraktsparten få en skriftlig bekräftelse från den andra parten om att den andra partens kontraktspart har fått ett intyg över säkerhetsutredning av företaget.

3. Vid öppna anbudsförfaranden får den mottagande partens behöriga säkerhetsmyndighet utan formell begäran överlämna de relevanta intygen över säkerhetsutredning av företaget till ursprungspartens behöriga säkerhetsmyndighet.

4. Säkerhetsutredning av företag krävs inte för säkerhetsklassificerade kontrakt i en säkerhetsklass som motsvarar den i artikel 4 i denna överenskommelse nämnda säkerhetsklassen "RESTRICTED".

5. Representanter 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.

6. Samtliga säkerhetsklassificerade kontrakt som ingår i enlighet med denna överenskommelse ska innehålla säkerhetskrav som tar hänsyn till följande:

- a) säkerhetsklassificeringsanvisningar,
- b) kontaktuppgifter till de behöriga säkerhetsmyndigheter som ansvarar för genomförandet av säkerhetsklassificerade kontrakt och för tillsynen över skyddet av säkerhetsklassificerad information med anknytning till överenskommelsen,
- c) lagar och bestämmelser som gäller skydd av säkerhetsklassificerad information,
- d) förfarandet och kraven för tillgång till säkerhetsklassificerad information,

in Article 4 of this Agreement, with a (Sub-)Contractor under the jurisdiction of the other Party, it shall first obtain written confirmation from the other Party that the Contractor has been granted a Facility Security Clearance.

3. In the case of an open tender the Competent Security Authority of the Receiving Party may provide the Competent Security Authority of the Originating Party with the relevant Facility Security Clearance certificates without a formal request.

4. A Facility Security Clearance is not required for Classified Contracts at the security classification level equivalent to "RESTRICTED" as mentioned in Article 4 of this Agreement.

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.

6. Every Classified Contract concluded in accordance with this Agreement shall include security requirements which identify the following aspects:

- a) a Security Classification Guide;
- b) contact details of the Competent Security Authorities responsible for implementing the Classified Contract and for overseeing the protection of Classified Information related to the Classified Contract;
- c) laws and regulations concerning the protection of Classified Information;
- d) procedure and requirements for access to Classified Information;
- e) handling and storing of Classified Information;

- e) hantering och lagring av säkerhetsklassificerad information,
- f) överföring och elektronisk förmedling av säkerhetsklassificerad information,
- g) märkning av säkerhetsklassificerad information,
- h) skyldighet att övervaka säkerhetsbeteenden och underrätta den nationella behöriga säkerhetsmyndigheten om eventuella informationssäkerhetsincidenter,
- i) skyddet av säkerhetsklassificerad information efter det att ett kontrakt har löpt ut,
- j) utplåning eller återlämnande av säkerhetsklassificerad information,
- k) utlämnande av uppgifter om ett säkerhetsklassificerat kontrakt.

7. Den behöriga säkerhetsmyndigheten för den part som godkänner ingåendet av ett säkerhetsklassificerat kontrakt ska sända en kopia av den del av kontraktet som gäller säkerhetskraven till den mottagande partens behöriga säkerhetsmyndighet för att underlätta tillsynen över säkerhetsaspekter i fråga om kontraktet.

8. När verksamhet som bygger på ett säkerhetsklassificerat kontrakt är förenad med besök av någondera partens personal i den andra partens land ska godkännandet av dessa besök ske i enlighet med de förfaranden som anges i artikel 10 i denna överenskommelse.

9. Om en kontraktspart låter en underleverantör genomföra delar av ett säkerhetsklassificerat kontrakt ska kontraktsparten och underleverantören säkerställa att denna artikel iakttas.

Artikel 8

Förmedling av säkerhetsklassificerad information mellan parterna

1. Säkerhetsklassificerad information förmedlas i enlighet med den utlämnande partens nationella lagar och bestämmelser eller på något annat sätt som avtalas mellan de behöriga säkerhetsmyndigheterna.

f) transportation and electronic transmission of Classified Information;

g) marking of Classified Information;

h) obligation to monitor security conduct and notify its Competent Security Authority in case of any Security Incident;

i) protection of Classified Information after termination of the Classified Contract;

j) destroying or returning of Classified Information;

k) release of information related to the Classified Contract.

7. The Competent Security Authority of the Party authorising the award of the Classified Contract shall forward a copy of the security requirements chapter, to the Competent Security Authority of the Receiving Party, to facilitate the security oversight of the contract.

8. The procedures for the approval of visits associated with Classified Contract activities by personnel of one Party to the other Party shall be in accordance with Article 10 of this Agreement.

9. If a Contractor sub-contracts parts of a Classified Contract, the Contractor and the Sub-contractor shall ensure the observance of this Article.

Article 8

Transmission of Classified Information between the Parties

1. Classified Information shall be transmitted in accordance with national laws and regulations of the Providing Party or as otherwise agreed between the Competent Security Authorities.

2. The Parties may electronically transmit Classified Information protected by crypto-

2. Parterna får i enlighet med de förfaranden som godkänts av de behöriga säkerhetsmyndigheterna elektroniskt förmedla säkerhetsklassificerad information som skyddas med krypteringssätt.

Artikel 9

Kopiering, översättning, och utplåning av säkerhetsklassificerad information

1. Kopior och översättningar av säkerhetsklassificerad information ska föras med märkning och skyddas på samma sätt som den ursprungliga säkerhetsklassificerade informationen.

2. Antalet översättningar och kopior ska begränsas till det minimum som användning enligt denna överenskommelse kräver och de får endast göras av personer som enligt nationella lagar och bestämmelser har rätt att få tillgång till säkerhetsklassificerad information i samma säkerhetsklass som den säkerhetsklassificerade information som översätts eller kopieras.

3. Översättningar ska föras med en lämplig märkning på översättningens språk om att de innehåller säkerhetsklassificerad information från den utlämnande parten.

4. Säkerhetsklassificerad information i en säkerhetsklass som motsvarar den i artikel 4 i denna överenskommelse nämnda säkerhetsklassen "TOP SECRET" får inte översättas eller kopieras utan ursprungspartens skriftliga samtycke.

5. Säkerhetsklassificerad information i en säkerhetsklass som motsvarar den i artikel 4 i denna överenskommelse nämnda säkerhetsklassen "TOP SECRET" får inte utplånas utan ursprungspartens skriftliga förhandssamtycke. Informationen ska återlämnas till ursprungsparten efter det att den utlämnande parten och den mottagande parten anser att informationen inte längre behövs.

graphic means in accordance with procedures to be approved by the Competent Security Authorities.

Article 9

Reproduction, translation and destruction of Classified Information

1. Reproductions and translations of Classified Information shall be marked and placed under the same protection as the original Classified Information.

2. Translations or reproductions shall be limited to the minimum required for use under this Agreement and shall be made only by individuals who are authorized in accordance with national laws and regulations to access Classified Information at the Security Classification Level of the Classified Information being translated or reproduced.

3. Translations shall contain a suitable annotation in the language in which they have been translated, indicating that they contain Classified Information of the Providing Party.

4. Classified Information marked at the Security Classification Level equivalent to "TOP SECRET" as mentioned in Article 4 of this Agreement, shall not be translated or reproduced without the prior written consent of the Originating Party.

5. Classified Information marked at the Security Classification Level equivalent to "TOP SECRET" as mentioned in Article 4 of this Agreement shall not be destroyed without the prior written consent of the Originating Party. It shall be returned to the Originating Party after it is no longer considered necessary by the Providing and Receiving Parties.

6. Classified Information marked up to and including the Security Classification Levels equivalent to "SECRET" as mentioned in Article 4 of this Agreement, shall be destroyed after it is no longer considered necessary by the Receiving Party, in accordance with its national laws and regulations.

6. Säkerhetsklassificerad information upp till och inklusive den i artikel 4 i denna överenskommelse nämnda säkerhetsklassen "SECRET ska utplånas i enlighet med nationella lagar och bestämmelser när den mottagande parten anser att informationen inte längre behövs.

7. 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 utan dröjsmål skriftligen underrätta den utlämnande partens behöriga säkerhetsmyndighet om att den säkerhetsklassificerade informationen har utplånats.

Artikel 10 *Besök*

1. För besök som förutsätter tillgång till säkerhetsklassificerad information i och högre än den i artikel 4 i denna överenskommelse nämnda säkerhetsklassen "CONFIDENTIAL" krävs skriftligt förhandssamtycke av den berörda behöriga säkerhetsmyndigheten, om inte de behöriga säkerhetsmyndigheterna sinsemellan avtalar om något annat.

2. Besökare ska minst fjorton dagar före den föreslagna tidpunkten för besöket lämna en begäran om besök till den behöriga säkerhetsmyndigheten, som förmedlar begäran till den andra partens behöriga säkerhetsmyndighet. I brådskande fall kan en begäran om besök lämnas inom en kortare tidsfrist, om de behöriga säkerhetsmyndigheterna kommer överens om detta på förhand.

3. Begäran om besök ska innehålla följande:

- a) besökarens hela namn, födelsedatum och födelseort, medborgarskap samt passets eller identitetskortets nummer,
- b) besökarens officiella befattning och namnet på den organisation som han eller hon företräder,
- c) bekräftelse av intyg över säkerhetsutredning av person som har utfärdats besökaren samt intygets giltighet,

7. If a crisis situation makes it impossible to protect Classified Information provided under this Agreement, the Classified Information shall be destroyed immediately. The Receiving Party shall notify promptly in writing the Competent Security Authority of the Providing Party about the destruction of this Classified Information.

Article 10 *Visits*

1. Visits requiring access to Classified Information at the level "CONFIDENTIAL" or above as mentioned in Article 4 of this Agreement are subject to the prior written consent of the respective Competent Security Authority, unless otherwise agreed between the Competent Security Authorities.

2. The visitor shall submit the request for visit at least fourteen days in advance of the proposed date of the visit to his Competent Security Authority, which shall forward it to the Competent Security Authority of the other Party. In urgent cases, the request for visit may be submitted at a shorter notice, subject to prior coordination between the Competent Security Authorities.

3. Request for visit shall include:

- a) full name of the visitor, date and place of birth, nationality and passport/ID card number;
- b) official title of the visitor and name of the organization the visitor represents;
- c) confirmation of the visitor's Personnel Security Clearance and its validity;
- d) date and duration of the visit. In the case of recurring visits the total period covered by the visits shall be stated;
- e) purpose of the visit and the anticipated Security Classification Level of Classified Information to be discussed or accessed;

d) besökets tidpunkt och längd. För upprepade besök ska hela den period under vilken besöken kommer att äga rum anges,

e) besökets syfte och säkerhetsklassen för den säkerhetsklassificerade information som sannolikt diskuteras med besökaren eller som han eller hon antas få tillgång till,

f) namn på och adress, telefonnummer, faxnummer och e-postadress till samt kontaktperson vid den anläggning som ska besökas,

g) daterad och stämplad underskrift av en företrädare för den behöriga säkerhetsmyndigheten i besökarens land.

4. De behöriga säkerhetsmyndigheterna kan sinsemellan komma överens om en förteckning över besökare som är berättigade till upprepade besök. De behöriga säkerhetsmyndigheterna ska sinsemellan komma överens om övriga detaljer i fråga om upprepade besök. Tillstånd för upprepade besök är dock giltiga i högst 12 månader.

5. Sådan säkerhetsklassificerad information som har lämnats till eller förvärvats av en besökare behandlas i enlighet med bestämmelserna i denna överenskommelse.

Artikel 11 *Informationssäkerhetsincident*

1. De behöriga säkerhetsmyndigheterna ska omedelbart skriftligen underrätta varandra om upptäckta eller misstänkta informationssäkerhetsincidenter som inkluderar säkerhetsklassificerad information.

2. Den mottagande parten ska omedelbart utreda den upptäckta eller misstänkta informationssäkerhetsincidenten. Ursprungspartens behöriga säkerhetsmyndighet ska vid behov samarbeta vid utredningen.

3. Den behöriga säkerhetsmyndigheten ska i enlighet med sina nationella lagar och bestämmelser vidta lämpliga åtgärder för att begränsa följderna av en informationssäkerhetsincident och förhindra att den upprepas. Ursprungspartens behöriga säkerhetsmyndighet ska

f) name, address, phone/fax number, e-mail address and point of contact of the facility to be visited;

g) dated and stamped signature of a representative of the visitor's Competent Security Authority.

4. The Competent Security Authorities may agree on a list of visitors entitled to recurring visits. The Competent Security Authorities shall agree on the further details of the recurring visits. However the validity of authorisations for recurring visits shall not exceed twelve (12) months.

5. Classified Information provided to or acquired by a visitor shall be treated in accordance with the provisions of this Agreement.

Article 11 *Security Incident*

1. The Competent Security Authorities shall immediately inform each other in writing of any actual or suspected Security Incident involving Classified Information.

2. The Receiving Party shall investigate immediately any actual or suspected Security Incident. The Competent Security Authority of the Originating Party shall, if required, cooperate in the investigation.

3. The Competent Security Authority shall take appropriate measures in accordance with its national laws and regulations to limit the consequences of the incident and to prevent a recurrence. The Competent Security Authority of the Originating Party shall be informed of the outcome of the investigation and, if any, of measures taken.

Article 12 *Costs*

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

dighet ska underrättas om resultatet av utredningen och om eventuella åtgärder som har vidtagits.

Artikel 12
Kostnader

Vardera parten ska stå för sina kostnader när de uppfyller förpliktelserna enligt denna överenskommelse.

Artikel 13
Twistlösning

Twister om tolkningen och tillämpningen av denna överenskommelse ska utslutande lösas genom samråd mellan parterna.

Artikel 14
Förhållande till andra överenskommelser

Denna överenskommelse ersätter inte sådana internationella överenskommelser som redan har ingåtts eller som eventuellt kan komma att ingås och som uttryckligen avser rättshandlingar som annars skulle omfattas av denna överenskommelse.

Artikel 15
Genomförandearrangemang

Parternas behöriga myndigheter får vidta genomförandearrangemang i enlighet med denna överenskommelse.

Artikel 16
Slutbestämmelser

1. Denna överenskommelse gäller tills vidare. Vardera parten ska via diplomatiska kanaler underrätta den andra parten när de nationella förfaranden som krävs för ikraftträdandet av denna överenskommelse har slutförts. Denna överenskommelse träder i kraft den första dagen i den andra månaden efter att den senare underrättelsen har tagits emot.

2. När det gäller Konungariket Nederländerna ska denna överenskommelse tillämpas på de delar av Nederländerna som är be-

Article 13
Dispute resolution

Any dispute on the interpretation or application of this Agreement shall be settled exclusively through negotiation between the Parties.

Article 14
Relation to other agreements

This Agreement does not prevail over any international agreement that has already been or may be entered into and that specifically governs a transaction otherwise governed by this Agreement.

Article 15
Implementing arrangements

The appropriate authorities of the Parties may conclude implementing arrangements pursuant to this Agreement.

Article 16
Final provisions

1. This Agreement is concluded for an indefinite period of time. Each Party shall notify the other Party through diplomatic channels once the national procedures necessary for entry into force of this Agreement have been completed. This Agreement shall enter into force on the first day of the second month following the receipt of the latter notification.

2. With regard to the Kingdom of the Netherlands, this Agreement shall apply to the European part of the Netherlands and the Caribbean part of the Netherlands (the islands of Bonaire, Sint Eustatius and Saba).

3. This Agreement, including its Annex, may be amended with the mutual consent of the Parties. Either Party may propose amendments to this Agreement, including its Annex, at any time through diplomatic channels. Such amendments shall enter into force under the conditions laid down in paragraph 1 of this Article, with the exception of an amendment of the Annex, which

lägna i Europa och de delar av Nederländerna som är belägna i Karibien (öarna Bonaire, Sint Eustatius och Saba).

3. Denna överenskommelse och dess bilagor kan ändras genom ömsesidigt samtycke mellan parterna. Vardera parten kan när som helst via diplomatiska kanaler föreslå ändringar i denna överenskommelse och dess bilaga. Ändringarna träder i kraft enligt de villkor som anges i artikel 1, med undantag av ändringar i bilagan, vilka träder i kraft vid en tidpunkt som parterna sinsemellan kommer överens om.

4. En part får när som helst skriftligen säga upp denna överenskommelse via diplomatiska kanaler. I sådana fall upphör överenskommelsen att gälla sex månader efter mottagandet av en sådan underrättelse.

5. Oavsett uppsägning av denna överenskommelse ska all information som har lämnats ut eller skapats inom ramen för överenskommelsen skyddas i enlighet med överenskommelsen så länge som informationen är säkerhetsklassificerad.

6. Efter det att denna överenskommelse har trätt i kraft ska Konungariket Nederländerna utan dröjsmål vidta åtgärder för att registrera överenskommelsen hos Förenta nationernas sekretariat i enlighet med artikel 102 i Förenta nationernas stadga.

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

Upprättad i Haag den 22 februari 2022 i två original exemplar på engelska.

För Republiken Finland

Päivi Kaukoranta

amendment shall enter into force on a date to be agreed upon by the Parties.

4. A Party may terminate this Agreement in writing at any time through diplomatic channels. In this case, the Agreement shall expire six months after receipt of such notification.

5. Regardless of the termination of this Agreement, all Classified Information released or generated under this Agreement shall be protected in accordance with this Agreement for as long as it remains classified.

6. After the entry into force of this Agreement, the Kingdom of the Netherlands shall take immediate measures to have the Agreement registered by the Secretariat of the United Nations in accordance with Article 102 of the Charter of the United Nations.

IN WITNESS whereof the duly authorised representatives of the Parties have signed this Agreement,

Done in the Hague on the 22nd day of February 2022 in two original copies, in the English language.

For the Republic of Finland

Päivi Kaukoranta

For the Kingdom of the Netherlands

Simone Smit

För Konungariket Nederländerna

Simone Smit