

Regeringens proposition till Riksdagen med förslag till godkännande av överenskommelsen mellan parterna i konventionen om upprättandet av Europeiska rymdorganet samt Europeiska rymdorganet om skydd för och utbyte av säkerhetsklassificerad information samt överenskommelsen mellan Finland och Tyskland om ömsesidigt skydd för säkerhetsklassificerad information samt med förslag till lagar om sättande i kraft av de bestämmelser i de nämnda överenskommelserna som hör till området för lagstiftningen till lag om internationella förpliktelser som gäller informationssäkerhet

PROPOSITIONENS HUVUDSAKLIGA INNEHÅLL

I denna proposition föreslås att riksdagen godkänner överenskommelsen med Europeiska rymdorganet (ESA) om skydd för och utbyte av av säkerhetsklassificerad information och överenskommelsen mellan Finland och Tyskland om ömsesidigt skydd för av säkerhetsklassificerad information samt antar lagar om sättande i kraft av dessa överenskommelser och en lag om internationella förpliktelser som gäller informationssäkerhet.

Syftet med överenskommelserna är att säkerställa rörligheten för och skyddet av sekretessbelagd information framförallt i samband med det europeiska rymdprogrammet. Det är fråga om känsligt informationsmaterial som i den sändande fördragsslutande staten eller internationella organisationen har av säkerhetsklassificerats på en hög säkerhetsnivå.

Det är viktigt att skydda informationen genom internationella avtalsarrangemang, dels med tanke på det aktuella europeiska rymdprogrammet och dels också på ett mera allmänt plan. Antalet multi- och bilaterala överenskommelser om informationssäkerhet förefaller öka. Detta beror dels på att olika funktioner i allt större utsträckning är beroende av information, som därigenom får en ökad betydelse, dels på det fördjupade och breddade internationella samarbetet. Den information som utbyts inom ramen för samarbetet måste kunna skyddas mot politiskt, militärt och ve-

tenskapligt-tekniskt-ekonomiskt spioneri samt mot annan obehörig användning.

ESA:s syfte är att förverkliga sådana storskaliga rymdprojekt som ligger utanför en enskild medlemsstats möjligheter. ESA och Europeiska unionen har avtalat om det gemensamma Galileoprogrammet som går ut på att bygga upp ett europeiskt signalsystem för positionsbestämning. Det europeiska systemet skall kunna användas i stället för eller parallellt med det amerikanska signalsystemet (GPS). Projektet anses ha en synnerligen stor strategisk betydelse för Europa, som för närvarande är beroende av ett system som USA har planerat och bestämmer om.

Galileoprojektet och dess genomförande är förenat med viktiga säkerhetssynpunkter och ekonomiska aspekter och har betydelse också för utvecklingen av den teknologiska kompetensen. Positionsbestämningssystemen samt informationen, kunskapen och beslutanderätten om dem har i många avseenden konsekvenser för samhällenas funktion och säkerhet. Genomförandet av programmet förutsätter sålunda oundvikligen hantering av känslig information som måste skyddas effektivt.

Galileoprojektet är nu inne i genomförandeskedet vilket innebär att anbudsgivningar under våren 2004 ordnas för branschföretag. I sådana delar av projektet som ger tillgång till känslig information kan endast delta företag från länder som har förbundit sig

att skydda av säkerhetsklassificerad information och vidta andra arrangemang för att trygga informationssäkerheten. Syftet med ESA-överenskommelsen är att trygga säkerhetsarrangemangen kring projektet. Överenskommelsen kan emellertid börja tillämpas fullt ut tidigast hösten 2004. I en del av ESA:s medlemsländer har det ansetts nödvändigt att bygga upp informationssäkerhetssystem som är baserade på bilaterala överenskommelser.

Med tanke på Finlands program för utveckling av informationssamhället måste det anses viktigt att finländska företag deltar i Galileoprojektet. I praktiken kan finländska företag delta i Galileoprogrammets anbudsgivningar i första hand som underleverantörer till tyska företag. Av denna anledning har det ansetts särskilt brådskande att Finland ingår en överenskommelse om informationssäkerhet med Tyskland.

Det ändamålsenligaste sättet att sätta i kraft de i regeringens proposition ingående överenskommelsernas bestämmelser i Finland är att stifta en särskild lag om internationella förpliktelser som gäller informationssäkerhet. Avsikten med lagen är att anpassa de internationella förpliktelserna till Finlands lagstiftning. Genom en särskild lag är det enkelt att sätta i kraft motsvarande överenskommelser också i framtiden.

De lagförslag som ingår i propositionen kan inte i sakligt hänseende anses innebära någon ändring av när det gäller handlingssekretessen i Finlands även om det i lagen föreslås en specialbestämmelse om sekretessbeläggning av handlingar som omfattas av de överenskommelser som föreslås bli satta i kraft. Det är fråga om information som i den sändande staten eller internationella organisationen betraktas som statshemligheter eller som klassificerad information eller som information vars obehöriga röjande annars strider mot nationella eller andra väsentliga allmänna intressen. Sådan information är i

praktiken sekretessbelagd redan enligt vår gällande lagstiftning.

Handlingar som avses i överenskommelsen skall av säkerhetsklassificeras och hänföras till särskilda säkerhetsklasser på ett sätt som tydligt anger avsändarens intention i fråga om sekretessen. Till det internationella samarbetets centrala principer hör att respektera en annan stats inom ramen för sin självbestämmanderätt uttryckta vilja att sekretessbelägga vissa handlingar. Finlands lagstiftning skyddar redan nu information vars röjande kan skada Finlands internationella relationer.

Enligt förslaget skall utrikesministeriet sköta uppgifterna som internationell säkerhetsmyndighet i samband med att de internationella förpliktelserna om informationssäkerhet fullgörs. Försvarsministeriet, huvudstaben och skyddspolisen skall enligt förslaget fungera som sådana utsedda säkerhetsmyndigheter som avses i de internationella förpliktelserna om informationssäkerheten. Detta arrangemang är inte avsett att vara permanent utan regeringen reder särskilt ut hur det är ändamålsenligast att sköta uppgifterna i framtiden.

Överenskommelsen mellan Finland och Tyskland träder i kraft femton dagar efter det att Finland har meddelat Tyskland att de nationella åtgärder som behövs för överenskommelsens ikraftträdande har vidtagits. Överenskommelsen med ESA träder för Finlands vidkommande i kraft trettio dagar efter det att Finland har deponerat sina ratifikations-, godtagande- eller godkännandeinstrument. Lagarna om ikraftsättande av överenskommelserna är avsedda att träda i kraft vid en tidpunkt som bestäms genom förordning av republikens president, samtidigt som överenskommelserna träder i kraft för Finlands del. Lagen om internationella förpliktelser som gäller informationssäkerhet är avsedd att träda i kraft så snart som möjligt efter att den har godkänts och stadfästs.

INNEHÅLLSFÖRTECKNING

PROPOSITIONENS HUVUDSAKLIGA INNEHÅLL	1
INNEHÅLLSFÖRTECKNING.....	3
ALLMÄN MOTIVERING.....	5
1. Inledning.....	5
1.1. Internationella krav på informationssäkerhet	5
1.2. Informationssäkerhetens betydelse inom det europeiska rymdsamarbetet	6
2. Nuläge	8
2.1. Offentlighetslagstiftningen.....	8
2.2. Lagen om säkerhetsutredningar	10
2.3. Styrning av informationssäkerheten inom statsförvaltningen	11
2.4. Tidigare överenskommelser och andra författningar som är bindande för Finland	11
3. Propositionens mål och de centrala förslagen.....	13
4. Propositionens verkningar	13
4.1. Verkningar för medborgarna.....	13
4.2. Verkningar för näringslivet.....	14
4.3. Ekonomiska verkningar	14
4.4. Administrativa effekter	14
5. Ärendets beredning	15
6. Andra omständigheter som inverkat på propositionens innehåll	15
DETALJMOTIVERING.....	17
1. Överenskommelsernas innehåll och förhållandet till Finlands lagstiftning	17
1.1. Överenskommelse mellan parterna i konventionen om upprättandet av Europeiska rymdorganet och Europeiska rymdorganet om skydd för och utbyte av säkerhetsklassificerad information	17
1.2. Överenskommelse mellan Finland och Tyskland om ömsesidigt skydd för av säkerhetsklassificerad information	19
2. Motivering av lagförslagen	22
2.1. Lag om sättande i kraft av de bestämmelser som hör till området för lagstiftningen i överenskommelsen mellan parterna i konventionen om upprättandet av Europeiska rymdorganet och Europeiska rymdorganet om skydd för och utbyte av säkerhetsklassificerad information	22
2.2. Lag om sättande i kraft av de bestämmelser som hör till området för lagstiftningen i överenskommelsen med Tyskland om ömsesidigt skydd för säkerhetsklassificerad information	22

2.3.	Lag om internationella förpliktelser som gäller informationssäkerhet ...	22
1 kap.	Allmänna bestämmelser.....	22
2 kap.	Säkerhetsmyndigheterna och samarbetet mellan dem	25
3 kap.	Åtgärder som gäller informationssäkerheten	26
4 kap.	Särskilda bestämmelser	30
5 kap.	Ikraftträdelsebestämmelser.....	31
3.	Närmare bestämmelser	31
4.	Ikraftträdande.....	31
5.	Riksdagens samtycke samt behandlings- och lagstiftningsordningen	32
5.1.	Riksdagens samtycke.....	32
5.2.	Behandlings- och lagstiftningsordning	34
LAGFÖRSLAG		35
	Lag om sättande i kraft av de bestämmelser som hör till området för lagstiftningen i överenskommelsen mellan parterna i konventionen om upprättandet av Europeiska rymdorganet och Europeiska rymdorganet om skydd för och utbyte av säkerhetsklassificerad information.....	35
	Lag om sättande i kraft av de bestämmelser som hör till området för lagstiftningen i överenskommelsen med Tyskland om ömsesidigt skydd för säkerhetsklassificerad information	35
	Lag om internationella förpliktelser som gäller informationssäkerhet.....	36
BILAGOR		41
	Bilaga 1: Överenskommelse mellan parterna i konventionen om upprättandet av Europeiska rymdorganet samt Europeiska rymdorganet om skydd för och utbyte av säkerhetsklassificerad information (översättning till svenska).....	41
	Bilaga 2: Överenskommelse mellan republiken Finlands regering och Tyska förbundsrepublikens regering om ömsesidigt skydd för säkerhetsklassificerad information	44

ALLMÄN MOTIVERING

1. Inledning

1.1. Internationella krav på informations-säkerhet

Det internationella samarbetet utvidgas och fördjupas på flera områden, t.ex. inom polisverksamheten, utrikes- och säkerhetspolitiken samt teknologiutvecklingen. Det internationella samarbetet baseras i allt större utsträckning på informationsutbyte mellan staterna samt mellan internationella organisationer och organ. Information, kompetens och patent samt informations- och dataöverföringssystem har fått en ökad betydelse som produktionsfaktorer. Obehörigt och kriminellt utnyttjande av dessa produktionsfaktorer är förenat med avsevärda säkerhetsrisker. Det fördjupade samarbetet innebär ett ökat utbyte av känslig information. Detta faktum i förening med den elektroniska databehandlingens och -överföringens sårbarhet har skapat behov av internationellt samordnade förfaranden för att trygga informationssäkerheten.

Utbyte av känslig information som äventyrar viktiga säkerhetsintressen förekommer inte endast i det mellanstatliga samarbetet, utan detta utbyte har betydelse också för näringsverksamheten t.ex. då en myndighet i samband med upphandling måste lämna ut sekretessbelagda uppgifter till företag som lämnar in anbud och fullföljer avtal. Detta är vanligen fallet vid upphandling av försvarsmateriel. I flera europeiska länder förutsätts det att företagets tillförlitlighet har utretts och att dess förmåga att trygga informationssäkerheten har fastställts. Om sådana utredningar saknas kan detta hindra företag från att delta i leveranser. Brister i detta avseende fungerar sålunda som faktiska handelshinder.

Med informationssäkerhet avses vanligen förfaranden som skyddar informationsinnehållet mot utomstående (informationens konfidentialitet), informationens oföränderlighet (informationens integritet) samt informatio-

nens användbarhet. För att trygga informationssäkerheten används olika metoder av vilka de vanligaste är kontroll av personalens tillförlitlighet och verksamhetsutrymmenas säkerhet, sekretessbestämmelser och begränsning av rätten att använda informationen endast för avtalade ändamål samt olika typer av procedurkrav när det gäller hantering och överföring av informationen. Dessa säkerhetskrav täcker informationens hela livscykel, med andra ord inhämtande, bearbetning, användning, överlåtelse, arkivering och utplåning av information.

Inom det internationella samarbetet förekommer dokument som innehåller sekretessbelagd information vars obehöriga röjande kan medföra betydande och omfattande skador på centrala allmänna intressen. Det är därför särskilt viktigt att denna typ av material behandlas särskilt omsorgsfullt. Finlands trovärdighet som part i det internationella samarbetet är bl.a. beroende av att gemensamt avtalade procedurregler iakttas. För att Finland skall ha möjlighet att delta i internationella teknologiska utvecklingsprogram och för att den finländska industrin skall kunna få beställningar från andra länder t.ex. på försvarssystem som är känsliga från säkerhetssynpunkt förutsätts det att Finland skyddar av säkerhetsklassificerad information samt kontrollerar företagets och de i projekten deltagande personernas tillförlitlighet.

Lagförslagen i regeringens proposition gäller i första hand sådana till finska myndigheter sända handlingar som har samband med internationell verksamhet samt annat informationsmaterial som är sekretessbelagt och klassificerat på en hög säkerhetsnivå uttryckligen för att skydda intressen som hänför sig till den allmänna säkerheten, försvaret och militära ärenden samt teknologiskt eller annat industriellt utvecklingsarbete. Behovet av denna proposition aktualiseras framförallt av överenskommelsen om informationssäkerheten inom Europeiska rymdorganet samt

av samarbetsprogrammet Galileo, som genomförs mellan organisationen och Europeiska unionen.

De internationella förpliktelserna om informationssäkerhet definieras på olika sätt inom de internationella organisationerna. Ett av de viktigaste internationella dokumenten som definierar principerna för utveckling av informationssäkerheten gäller de principer för informationssäkerhet som Organisationen för ekonomiskt samarbete och utveckling (OECD) fastställde år 1992. Europeiska unionens bestämmelser om dokumentssäkerhet medför förpliktelser också för medlemsstaterna.

Det militära samarbetet är av tradition ett område där av säkerhetsklassificerat material hanteras. Inom den nordatlantiska försvarsorganisationen (NATO) och Västeuropeiska unionen (VEU) gäller ytterst noggranna och detaljerade bestämmelser om informationssäkerhet. Försvarsförvaltningen har ingått bilaterala överenskommelser som närmast kan karakteriseras som internationella förvaltningsavtal med vissa länders försvarsförvaltningar om informationsutbyte och säkerhetsåtgärder.

Det är på det hela taget uppenbart att Finland måste förbättra sin beredskap att på det internationella planet skydda känsligt informationsmaterial och vidta därtill anslutna säkerhetsåtgärder. Detta förutsätter enligt regeringens uppfattning att det stiftas en allmän lag om saken.

1.2. Informationssäkerhetens betydelse inom det europeiska rymdsamarbetet

Europeiska rymdorganet (ESA) upprättades den 31 maj 1975. Organisationen skall samordna de europeiska staternas insatser för utforskning och användning av rymden för fredliga ändamål. Organisationen strävar framförallt efter att utveckla rymdteknologin och dess tillämpningar såväl för vetenskapliga ändamål som för praktiska syften. Avsikten är att genomföra sådana storskaliga rymdprojekt som ligger utanför en enskild medlemsstats möjligheter. Vidare ger organisationen medlemsstaterna rekommendationer om en enhetlig industripolitik inom rymdområdet. Finland var associerad medlem i orga-

nisationen från år 1987 till 1995, då Finland blev fullvärdig medlem.

Europeiska rymdorganet har för närvarande sammanlagt 15 medlemmar: Frankrike, Tyskland, Storbritannien, Italien, Spanien, Österrike, Schweiz, Belgien, Nederländerna, Danmark, Sverige, Norge, Irland, Portugal och Finland. Organisationen har också associationsavtal med bl.a. Kanada. Finland deltar inom ramen för ESA:s vetenskapsprogram i byggandet av satelliter och instrument för rymdforskningen samt dessutom i teknologiprogram som stöder datakommunikation och satellitkartläggning.

Europeiska rymdorganets forsknings- och utvecklingsprojekt ger Finland mångsidiga möjligheter att delta i kvalificerade och högklassiga internationella samarbetsprojekt inom vetenskapens och teknologins område. Efter att Finland anslutit sig till organisationen som fullvärdig medlem har det i vårt land vuxit fram ett nätverk av företag och forskningsinstitut som kan genomföra krävande projekt både inom rymdforskning och inom tillämpad rymdteknologi. ESA-medlemskapet har inneburit ett uppsving också för den industriella och kommersiella aktiviteten inom rymdområdet.

Galileo är ett samarbetsprojekt mellan Europeiska rymdorganet och Europeiska unionen för planering och uppbyggnad av ett satellitsystem för positionsbestämning. Avsikten är att bygga upp ett system med bl.a. 30 satelliter samt med markstationer, stödstationer, användarsegment och lokala segment för produktion av olika former av kundservice. Eftersom Galileosystemet kommer att producera information för exakt positionsbestämning och får det en synnerligen stor strategisk betydelse för civilförvaltningen. Systemet omfattar också militärt relevant teknologisk information och know-how bland annat om satellitmodeller, krypteringssystem och mikroretsar, som kan vara farlig i händerna på fientliga parter. Den information som systemet producerar ökar precisionen och effektiviteten samt ger ett logistiskt stöd för olika typer av kommunikation samt kontroll- och kommandofunktioner.

Den ekonomiska betydelsen av system som bygger på satellitnavigeringssignaler ökar snabbt. Det anses vara strategiskt viktigt för

Europa att de europeiska terminaltillverkarna och serviceproducenterna blir oberoende av den amerikanska GPS-signalen. Även om GPS-signalen är tillgänglig för alla har Europa inga möjligheter att påverka systemets utveckling, precision eller förvaltning. Ett avbrott i GPS-signalen skulle få omfattande ekonomiska konsekvenser i Europa. Avsikten är att utveckla Galileosystemet så att det blir kompatibelt med det amerikanska satellitsystemet för positionsbestämning.

Satellitnavigeringssystemet Galileo stöder utvecklingen av det för Finland viktiga informationssamhället. Enligt vissa källor är positions- eller Ortsbestämning relevant för 80-90 procent av all information. Ett satellitbaserat system möjliggör en exakt positionsbestämning. Det kan utnyttjas yrkesmässigt t.ex. för navigationsanläggningar i bilar. Marknaden för ett globalt satellitbaserat positionsbestämningssystem beräknas inom några år uppgå till sammanlagt 5-10 miljarder euro. Mobiltelefoner med satellitbaserad positionsbestämning väntas på ett avgörande sätt bidra till marknadens tillväxt. Genom att en positionsbestämningssystem byggs in t.ex. i mobiltelefoner blir satellitsignalerna blir en central resurs och positionsbestämningen läggs till grund för många nya serviceformer. I ett internationellt perspektiv har den finländska industrin visat sig vara synnerligen konkurrenskraftig inom detta område.

Finländska företag är intresserade av att bygga satelliter och marksegment samt framförallt terminaler och tillämpningar. Enligt projektets tidtabell är byggandet av satelliter just nu mest brådskande. Utvecklingen av tillämpningar och terminaler stöds också genom nationella program. Teknologiska utvecklingscentralen (Tekes) har de två senaste åren anslagit 17 miljoner euro för finansiering av ett projekt för utredning av 77 delfrågor som gäller positionsbestämningssystem.

Företag och institutioner i alla ESA:s och EU:s medlemsländer har möjlighet att delta i Galileoprogrammet. Installationen och driften av systemet kräver stor omsorgsfullhet vid informationshanteringen samt nationellt godkända förfaranden för administrationen av säkerhetsklassificerad information. Härav följer att de medlemsländer som vill vara

med om installationsfasen och driftsfasen måste följa de i gemensamma överenskommelser fastställda reglerna och principerna för hantering av Galileoprogrammets informationsmaterial, för säkerhetsklassificering av handlingar samt för säkerhetsutredningar som gäller företag, institutioner och personer.

Parterna i konventionen om upprättandet av Europeiska rymdorganet har med Europeiska rymdorganet ingått en överenskommelse om skydd för och utbyte av av säkerhetsklassificerad information (ESA-överenskommelsen om informationssäkerhet). Överenskommelsen har karaktären av ett generellt ramavtal, jämfört med flertalet andra internationella dokument om informationssäkerhet. Överenskommelsen tillämpas vartefter medlemsländerna undertecknar och ratificerar den.

Eftersom ratificeringen av ESA-överenskommelsen om informationssäkerhet inte ännu är klar kan finländska företag inte delta i Galileoprojektets anbudsomgång denna vår, till den del som det är fråga om av säkerhetsklassificerat material. Eftersom ESA-överenskommelsen om informationssäkerhet inte ännu fungerar mellan alla medlemsländer och eftersom flera medlemsländer anser att överenskommelsen inte är tillräckligt täckande, tillämpar en del av organisationens medlemsländer delvis ett nätverk av redan existerande bilaterala eller multilaterala överenskommelser. Till dessa länder hör bl.a. Frankrike, Tyskland, Italien, Nederländerna, Spanien, Sverige och Storbritannien. Endast företag i dessa länder kan fullt ut delta i anbudsomgången. Separata överenskommelser mellan medlemsstater kommer sannolikt att permanent behövas vid sidan av ESA-överenskommelsen om informationssäkerhet, på grund av att denna inte anses vara heltäckande. För att Finland skall ha möjlighet att fullt ut delta i Galileoprojektet förfaller det vara nödvändigt att Finland ingår överenskommelser med och avtalar om säkerhetsarrangemang med alla länder som vill delta i Galileoprojektet.

För närvarande är projektet inne i en fas av preliminära utredningar som finländarna har möjlighet att delta i. I april 2004 inleds själva projektfasen (Galileo Overall IOV System) som är avgörande för hela installationen och som det är ytterst viktigt för finländska före-

tag att delta i. I denna fas har finländska industriföretag i praktiken möjlighet att delta närmast som underleverantörer till tyska företag. Det anses därför nödvändigt att i brådskande ordning ingå en bilateral överenskommelse om informations säkerhet med Tyskland. I ett senare skede förs förhandlingar om bilaterala överenskommelser med andra länder som deltar i Galileoprojektet. Den i regeringens proposition föreslagna lagen om internationella förpliktelser som gäller informationssäkerhet förenklar ikraftsättandet av eventuella senare överenskommelser.

2. Nuläge

2.1. Offentlighetslagstiftningen

Den rättsliga grunden för informations säkerheten i Finland utgörs framförallt inom statsförvaltningen av lagen om offentlighet i myndigheternas verksamhet (621/1999, nedan offentlighetslagen) och den med stöd av lagen utfärdade förordningen om offentlighet och god informationshantering i myndigheternas verksamhet (1030/1999, nedan offentlighetsförordningen).

Offentlighetsprincipen har en central betydelse inom förvaltningen i Finland. Den är också viktig för avgöranden och förfaranden som avser myndigheternas information. Offentlighet är huvudregeln som kompletteras av de i lagen angivna sekretessgrunderna. Information skall sekretessbeläggas i syfte att skydda vissa allmänna och enskilda intressen.

Enligt grundlagen har var och en rätt att få information om myndigheters offentliga handlingar. Handlingsoffentligheten kan då det är nödvändigt begränsas endast genom lag. Begränsningen har i enlighet med grundlagen och de principer som grundlagsutskottet omfattat i sin tolkningspraxis genomförts på så sätt i offentlighetslagen att en klausul om skaderekvisit har tagits in framförallt i sekretessbestämmelser som skyddar allmänt intresse. Det är också skäl att observera att sekretessplikten kan gälla endast en del av en handling. Enligt offentlighetslagens 10 § skall i så fall uppgifter i den offentliga delen lämnas ut.

Att en sekretessbestämmelse innehåller en klausul om skaderekvisit betyder att sekretessen är beroende av vilka konsekvenser det skulle få för det skyddade intresset om uppgiften lämnades ut. De gällande sekretessbestämmelserna leder sålunda till prövning i det enskilda fallet, som i förening med lagens tolkningsbestämmelser och rättspraxis förpliktar myndigheten att i det enskilda fallet motivera varför ett utlämnande av uppgifterna skulle ha sådana konsekvenser som avses i lagrummet. En sådan reglering är inte ändamålsenlig när det är fråga om av säkerhetsklassificerad information som i enlighet med en internationell överenskommelse eller författning har fått från andra stater eller internationella organ.

I offentlighetslagen föreskrivs om god informationshantering. En god informationshantering inbegriper enligt lagen också åtgärder för att hemlighålla handlingar samt se till att de är integrerade och användbara. En god informationshantering innebär att myndigheten skall se till att dess handlingar och datasystem samt uppgifterna i dem är behörigen tillgängliga, användbara, skyddade och integrerade samt sörja även för andra omständigheter som påverkar kvaliteten på uppgifterna.

Offentlighetsförordningen innehåller bestämmelser om klassificering av särskilt känsligt material. Enligt förordningen ankommer den konkreta klassificeringen av informationsmaterial i första hand på vederbörande myndighet själv. Detta är naturligt eftersom myndigheten också i andra avseenden svarar för att dess verksamhet är laglig och ändamålsenlig. Principen har skrivits in i offentlighetsförordningens 2 §, enligt vilken en myndighet själv kan klassificera sina handlingar och datasystem samt uppgifter som ingår i dem i syfte att beakta de krav på hantering och skydd som skall uppfyllas samt andra krav på datasäkerhet.

Klassificeringen av särskilt känsligt data-material omfattar sekretessbelagda handlingar och uppgifter i dem vilkas överlåtelse av någon annan orsak begränsas i lag eller som enligt lagen endast får användas för ett bestämt ändamål (offentlighetsförordningens 2 §). Materialet kan indelas i tre klasser enligt de krav på hantering, skydd och annan

datasäkerhet som skall uppfyllas vid sammanställning, ändring, användning, överlåtelse, överföring, arkivering, utplåning och annan hantering av datamaterialet. Materialet kan indelas också i flera klasser om det finns särskilda behov av sådana inom myndighetens förvaltningsområde.

Till den första klassen ("ytterst hemlig") av särskilt känsligt datamaterial kan hänföras datamaterial som innehåller uppgifter som olagligt avslöjade och använda skulle medföra allvarlig skada för de allmänna intressen som avses i 24 § 1 mom. 1, 2, 5 samt 8 – 11 punkten i offentlighetslagen. Till denna kategori av skyddade intressen hör Finlands internationella relationer, förebyggande och utredning av brott, allmän ordning och säkerhet, befolkningskydd, statens säkerhet och försvarets intressen.

Till den andra klassen ("hemlig") av särskilt känsligt datamaterial kan hänföras datamaterial som innehåller uppgifter som olagligt avslöjade och använda skulle medföra väsentlig skada för de intressen som föranlett begränsningarna i fråga om överlåtelse. Denna klassificering är sålunda inte beroende av de intressen för vilka datamaterialet har sekretessbelagts.

Till den tredje klassen ("konfidentiell") av särskilt känsligt datamaterial kan hänföras datamaterial som innehåller uppgifter som olagligt avslöjade och använda skulle äventyra en myndighets verksamhetsförutsättningar eller affärs- eller yrkeshemligheter eller skyddet av personuppgifter.

I offentlighetsförordningen ingår för närvarande inga detaljerade bestämmelser om vilka konkreta åtgärder som krävs för att trygga datasäkerheten i de olika klasserna. I offentlighetsförordningens 3 § ingår emellertid bestämmelser om allmänna säkerhetsåtgärder i fråga om särskilt känsligt datamaterial. Bestämmelsen gäller sålunda också annat särskilt känsligt datamaterial än sådant som har klassificerats.

När handlingar som har klassificerats som särskilt känsligt datamaterial upprättas, hanteras, deponeras, överläts och utplånas skall enligt offentlighetsförordningen på motsvarande sätt som vid klassificeringen vidtas åtgärder för att skydda handlingarna och uppgifterna i dem på ett sådant sätt att den i för-

ordningen fastställda målnivån uppnås. Målnivån innebär att det ställs krav på att de lokaler där materialet hanteras och förvaras är tillräckligt övervakade och skyddade. Också tillgången till datasystemen skall övervakas och olovligt intrång i systemen förhindras med de medel som står till buds. Datamaterialet får ändras och hanteras i övrigt enbart av personer som har befogenhet att handlägga ett ärende. Rätten att använda materialet skall också annars begränsas på ett ändamålsenligt sätt och användningen övervakas i tillräcklig utsträckning. Uppgifter ur särskilt känsligt datamaterial får lämnas ut endast av personer som har befogenhet att göra det och information som överförs via datanätet skall vid behov krypteras.

Förpliktelserna regleras genom flexibla normer. Myndigheterna skall emellertid se till att de grundläggande kraven uppfylls och att särskilt känslig information är tillgänglig endast för personer vilkas tjänsteåligganden förutsätter detta.

Finansministeriets avdelning för utvecklande av förvaltningen har utfärdat allmänna anvisningar som kompletterar offentlighetsförordningens bestämmelser om datasäkerhet. Av särskilt intresse för denna proposition är principerna om hantering av känsligt internationellt datamaterial inom statsförvaltningen, som år 2002 publicerades av ledningsgruppen för datasäkerhet inom statsförvaltningen (Ledningsgruppen för datasäkerhet inom statsförvaltningen 4/2002). Det konkreta arbetet med att utveckla datasäkerheten inom statsförvaltningen har bl.a. till följd av den snabba teknologiska utvecklingen framskridit genom att man i första hand använt informationsstyrning i stället för bindande bestämmelser.

Anteckningar om sekretess och av klassificering är direkt med stöd av lagen obligatoriska endast i vissa situationer, när sekretessbelagda handlingar överlämnas till en part. I övrigt är det enligt lagens 25 § frivilligt att göra sådana anteckningar. Enligt offentlighetslagen kan emellertid genom förordning av statsrådet bestämmas om bindande förpliktelser att göra anteckningar om datasäkerhet. Denna möjlighet har hittills inte använts.

De internationella och delvis också de na-

tionella bestämmelserna och förfarandena som gäller informationssäkerhet har redan länge varit oberoende av offentlighetsbestämmelserna. Från Finlands lagstiftnings synpunkt kan det konstateras att en anteckning om informations säkerhet eller sekretess inte ännu som sådan avgör om information kan ges ut om en handling. Den som har ombetts att lämna ut handlingen måste avgöra ärendet på det sätt som föreskrivs i offentlighetslagen. Sålunda måste bl.a. tolkningsprinciperna i offentlighetslagens 17 § beaktas liksom även den omständigheten att när endast en del av en handling är offentlig skall uppgifter om den lämnas ut på det sätt som föreskrivs i offentlighetslagens 10 §.

Såväl med tanke på offentlighetsprincipen som med tanke på informationssäkerheten är det skäl att ytterligare beakta en myndighets skyldighet att ge anvisningar samt övervaka och följa upp ärenden. I offentlighetslagens 18 § föreskrivs om dessa allmänna förpliktelser. Enligt offentlighetsförordningens 4 § skall myndigheten bl.a. fästa avseende vid att beslutanderätten när det gäller utlämnande av handlingar fastställs samt vid att tillräckliga anvisningar utfärdas om registrering av ärenden och handlingar samt om hantering och skydd av handlingar, datasystem och uppgifterna i dem under olika behandlingsstadier. Myndigheterna skall i tillräcklig utsträckning övervaka att anvisningarna följs och åtgärderna vidtas samt med lämpliga intervaller bedöma deras ändamålsenlighet och behovet av ändringar samt vidta åtgärder för att rätta till de brister som konstaterats.

Inom ramen för den gällande lagstiftningen är det i någon mån oklart hur långt det med stöd av bemyndigandena i offentlighetslagen är möjligt att föreskriva om lokalers säkerhet. Ärendet utreds separat som en del av justeringen av offentlighetslagen, så som framgår av statsrådets redogörelse om verkställigheten av den nya offentlighetslagstiftningen (SRR 5/2003 rd).

2.2. Lagen om säkerhetsutredningar

I lagen om säkerhetsutredningar (177/2002) föreskrivs om säkerhetsutredningar som avser personer. Syftet med lagen är att genom säkerhetsutredning öka möjlig-

heterna att förebygga brott som medför allvarlig fara för centrala allmänna intressen (Finlands inre och yttre säkerhet, försvar eller beredskap för undantagsförhållanden, Finlands relationer till andra stater och internationella organisationer, den offentliga ekonomin) eller för enskilda intressen (affärs- eller yrkeshemligheter och andra synnerligen betydande enskilda ekonomiska intressen) och likaså datasäkerhet som är av synnerligen stor betydelse för skyddet av de i lagen angivna intressena.

En person som söker en tjänst eller ett uppdrag, skall anställas eller antas till utbildning eller som sköter en tjänst eller ett uppdrag, kan göras föremål för en säkerhetsutredning. Skyddspolisen beslutar om en säkerhetsutredning skall göras. Om sökanden hör till försvarsförvaltningen eller sköter ett uppdrag på förordnande av försvarsförvaltningen, är det dock huvudstaben som beslutar om en säkerhetsutredning skall göras. Beslut om en begränsad säkerhetsutredning fattas av polisrättningen i häradet på den ort där den plats eller det utrymmen som ansökan gäller finns, om det inte är frågan om en plats eller ett utrymme som är i försvarsmaktens besittning.

Det finns tre typer av säkerhetsutredning, nämligen normal, omfattande och begränsad. En normal säkerhetsutredning kan sökas av statens och riksdagens myndigheter och inrättningar, av statliga affärsverk, kommuner och samkommuner, av privata sammanslutningar och stiftelser som har stadseenligt hemvist, sin centralförvaltning eller sin huvudsakliga verksamhet i Finland samt av utländska sammanslutningar och stiftelser som har en registrerad filial i Finland. En säkerhetsutredning kan göras också på begäran av en sökande, om ett fördrag eller någon annan internationell förpliktelse som är bindande för Finland förutsätter det.

Utredningsförfarandet innebär att de säkerhetsintressen som är förenade med organisationer som är viktiga för statens och samhällets funktion samordnas med de krav som individens dataskydd ställer. Säkerhetsutredningarna har betydelse för individens grundläggande fri- och rättigheter.

Eftersom rätten till personlig integritet har karaktären av en grundläggande rättighet är förfarandet med säkerhetsutredning strikt

formbundet. En säkerhetsutredning kan göras endast med vederbörandes på förhand givna, uttryckliga och skriftliga samtycke. Också de register som kan användas vid utredningsförfarandet räknas uttömmande upp i lagen, på grund av kravet på en exakt avgränsning av förutsättningarna för inskränkning av grundläggande fri- och rättigheter. Den behöriga myndigheten får enligt begränsningsbestämelsen i lagens 3 § utnyttja register endast i den omfattning som nödvändigtvis krävs för att syftet med lagen skall kunna uppnås. Avsikten är inte att registren skall utnyttjas fullt ut för varje utredning, utan registerurvalet utökas i den mån som det är möjligt att i något register hämta tilläggsinformation om den person som är föremål för utredning.

Var och en har rätt att få upplysningar om huruvida en säkerhetsutredning som gäller honom eller henne har gjorts med tanke på ett visst uppdrag. Den som utredningen gäller har rätt att av den behöriga myndigheten på begäran få de uppgifter som en omfattande eller begränsad utredning innehåller om honom eller henne. Denna rätt gäller emellertid inte sådan ur ett register hämtad information som en registrerad inte har rätt till insyn i.

2.3. Styrning av informationssäkerheten inom statsförvaltningen

Såsom konstateras ovan i avsnitt 2.2. kompletteras de åtgärder som gäller informationssäkerhet inom statsförvaltningen av de allmänna styrningsåtgärder som vidtas av finansministeriets avdelning för utvecklande av förvaltningen. Ministeriet har tillsatt en ledningsgrupp för datasäkerheten inom statsförvaltningen (VAHTI). Denna organiserar samarbetet i datasäkerhetsärenden samt förbereder ärenden som gäller utvecklig och styrning av området.

Under ledning av finansministeriet har utarbetats ett program för utveckling av datasäkerheten inom statsförvaltningen. Avsikten med programmet är att ytterligare effektivisera åtgärderna för att utveckla datasäkerheten inom förvaltningen. Genom finansministeriets försorg har ett heltäckande nationellt regelverk för datasäkerhet byggts upp. Som ett exempel kan nämnas regelverkets anvis-

ning om hantering av känsligt datamaterial. Anvisningen innehåller detaljerade beskrivningar av vilka åtgärder som skall vidtas vid hantering av internationellt material i olika säkerhetsklasser.

Utgående från finansministeriets regelverk har utfärdats särskilda anvisningar och föreskrifter för olika ämbetsverk och förvaltningsområden. I synnerhet inom utrikes- och försvarsförvaltningen har utfärdats detaljerade anvisningar och föreskrifter för internationellt datasäkerhetsarbete. Som exempel kan nämnas huvudstabens anvisning om säkerhet med avseende på försvarsmaktens referensgrupper (22.12.2003, 44/12.5./D/I), som bl.a. gäller informationssäkerheten i samband med leveransavtal som att sekretessbelagd information lämnas ut till den andra avtalsparten. Anvisningarna anger när en säkerhetsutredning av en enskild avtalspart skall göras samt hur säkerhetsåtgärderna skall genomföras.

2.4. Tidigare överenskommelser och andra författningar som är bindande för Finland

De länder som deltar i programmet Partnerskap för fred (PfP) har med den nordatlantiska försvarsorganisationen (NATO) avtalat om hanteringen av PfP-handlingar. Finland och NATO undertecknade den 22 september 1994 i Bryssel en överenskommelse om informationsutbyte och dokument inom ramen för programmet Partnerskap för fred. Överenskommelsen upprättades på basis av NATO-ländernas gemensamma säkerhetsavtal och undertecknandet av överenskommelsen var en förutsättning för att NATO överlämnar av säkerhetsklassificerade dokument till Finland.

Finland och Västeuropeiska unionen (VEU) ingick den 22 april 1997 ett säkerhetsskyddsavtal (FördrS 42/1998). I avtalet föreskrivs om parternas skyldighet att säkra och skydda sekretessbelagd information och sekretessbelagt material som överlämnats av endera parten. Avtalsparterna skall bibehålla en sekretessgrad som fastställts av den andra parten samt skydda informationen och materialet i enlighet med detta. Enligt avtalet skall parterna inte använda informationen

och materialet för annat ändamål än det som fastställts av den som informationen utgår från och för vilket informationen har utbyttts.

Enligt avtalet har Finland förbundit sig att för de ändamål som anges i avtalet utse en nationell säkerhetsmyndighet (National Security Authority, NSA) som har till uppgift att svara för skyddet av VEU-handlingar som innehas av nationella myndigheter samt bl.a. för bedömning av säkerhetsarrangemangens effektivitet. Finlands nationella säkerhetsmyndighet är utrikesministeriet. Utsedda säkerhetsmyndigheter (Designated Security Authority, DSA) är försvarsministeriet, inrikesministeriet samt handels- och industriministeriet, vilka svarar för informationssäkerheten inom sina respektive verksamhetsområden på det sätt som VEU:s bestämmelser om informationssäkerhet förutsätter. De utsedda säkerhetsmyndigheterna har enligt de till avtalet anslutna säkerhetsbestämmelserna till uppgift att informera industrin om säkerhetspolitiken, ge handledning och bistå i verkställighetsfrågor samt vidta säkerhetsåtgärder i samband med leveranser och underleveranser inom VEU, t.ex. fastställa sekretessgrader.

Avtalet sattes i kraft genom en särskild lag (282/1998). Lagen innebär ett undantag från den allmänna lagstiftningen. Den innehåller nämligen specialbestämmelser enligt vilka informationsmaterial som har upprättats för i avtalet avsett samarbete och som har fått sekretessgradering på det sätt som avtalsarrangemangen kräver, skall hållas hemligt. På VEU:s handlingar tillämpas VEU:s bestämmelser om informationssäkerhet.

Europaparlamentets och rådets förordning (EG) nr 1049/2001 om allmänhetens tillgång till Europaparlamentets, rådets och kommissionens handlingar (nedan öppenhetsförordningen) gavs den 30 maj 2001. I öppenhetsförordningens artikel 9 definieras begreppet känsliga handlingar. Dessa placeras i de tre högsta säkerhetsklasserna och är sekretessbelagda för att skydda medlemsstaternas väsentliga intressen i synnerhet när det gäller allmän säkerhet, försvar och militära frågor. Känsliga handlingar kan härröra från unionens institutioner eller organ eller från medlemsstaterna samt även från internationella organisationer, t.ex. NATO.

Medlemsstaterna skall enligt förordningen vidta lämpliga åtgärder för att säkerställa att de principer respekteras vid behandlingen av ansökningar om tillgång till känsliga handlingar som ingår i specialbestämmelser om EU:s känsliga handlingar samt i bestämmelser som begränsar tillgång till information.

Rådet fattade i mars 2001 beslutet 2001/264/EG om antagande av rådets säkerhetsbestämmelser. Beslutet har ett vidsträckt tillämpningsområde då det utöver säkerhetsbestämmelser för handlingar innehåller också bestämmelser om bl.a. personers och byggnaders säkerhet samt om andra omständigheter som har samband med informationssäkerhet. Beslutet påverkar inte tillämpningen av den artikel i grundfördraget som definierar handlingsoffentligheten, dvs. artikel 255 och dess genomförandeinstrument, och inte heller gällande praxis i medlemsstaterna när det gäller information till de nationella parlamenten om unionens verksamhet. Medlemsstaterna skall enligt beslutet vidta lämpliga åtgärder så att det, i enlighet med nationella ordningar, vid hantering av sekretessbelagda EU-uppgifter säkerställs att säkerhetsbestämmelserna respekteras av medlemsstaternas myndigheter och i deras lokaler av de anställda. Åtgärderna skulle enligt beslutet vara genomförda senast den 30 november 2001 och generalsekretariatet skulle informeras om de åtgärder som vidtagits. Beslutet om de nationella åtgärderna med anledning av säkerhetsbestämmelserna fattades 14.11.2001 av regeringens kommitté för EU-ärenden. Till den nationella säkerhetsmyndighet som avses i säkerhetsbestämmelserna utsågs utrikesministeriet.

Säkerhets- och riskhanteringsärenden har för närvarande en annan betydelse i unionens verksamhet än tidigare, vilket förklarar regleringen av både handlingssäkerheten och bestämmelserna om känsliga handlingar. Regleringsbehovet har sålunda motiverats bl.a. med förutsättningarna för ett konfidentiellt informationsutbyte med NATO: ett fördjupat samarbete och utvecklingen av en gemensam säkerhetspolitik förutsätter adekvata säkerhetsarrangemang.

Medlemsstaterna skall enligt EU:s öppenhetsförordning vidta lämpliga åtgärder för att se till att principerna i förordningen respekte-

ras vid behandling av ansökningar om och tillgång till känsliga handlingar. Beslutet om rådets säkerhetsbestämmelser förutsätter att medlemsstaterna vidtar lämpliga åtgärder så att det vid hanteringen av sekretessbelagd EU-information säkerställs att säkerhetsbestämmelserna respekteras av de anställda vid medlemsstaternas myndigheter och i deras lokaler. Till denna personkategori hör bl.a. de anställda vid medlemsstaternas ständiga representationer vid Europeiska unionen och vid de nationella delegationer som deltar i rådsmöten eller i möten i rådsorgan samt utomstående uppdragstagare.

Inom försvarsministeriets förvaltningsområde har med olika stater ingåtts överenskommelser, rubricerade som samförståndsdocument, om skyddande av sekretessbelagda uppgifter. Dessa överenskommelser kan närmast karakteriseras som internationella förvaltningsavtal. Avsikten är att dessa överenskommelser skall ombildas till statsfördrag och att det på det sätt som grundlagen förutsätter skall behandlas av riksdagen.

3. Propositionens mål och de centrala förslagen

Syftet med propositionen är att skapa förutsättningar för Finland att agera som en tillförlitlig internationell samarbetspartner i situationer där samarbetet förutsätter utbyte av känsliga handlingar och informationsmaterial som är sekretessbelagda i den andra fördragsslutande staten eller hos ett internationellt organ. Genom de överenskommelser som avses i propositionen blir det möjligt för finländska industriföretag att delta i utvecklingen av rymdteknologi.

I propositionen föreslås att de överenskommelser om informationssäkerhet sätts i kraft som har ingåtts med Europeiska rymdorganet och Tyska förbundsrepubliken. Det kommer uppenbarligen att finnas ett behov att ingå liknande internationella överenskommelser också i framtiden. I syfte att för enkla ikraftsättandet av dessa överenskommelser samt för att säkerställa transparensen i lagstiftningen föreslås att en särskild lag stiftas om de internationella förpliktelserna som gäller informationssäkerhet.

4. Propositionens verkningar

4.1. Verkningar för medborgarna

Det mest ändamålsenliga sättet att sätta i kraft de internationella förpliktelserna om informationssäkerhet är att stifta en särskild lag om saken. Denna föreslås innehålla en uttrycklig bestämmelse om den andra avtalspartens sekretessbelagda och av säkerhetsklassificerade handlingar samt om informationen i dem. Enligt förslaget skall sådan information vara sekretessbelagd också i Finland. Till sin utformning skiljer sig bestämmelsen från vad som i offentlighetslagen föreskrivs om sekretessbeläggning i allmänt intresse, eftersom sekretessen i de flesta fall är beroende av de verkningar som det skulle få för det skyddade intresset om uppgifterna lämnades ut. Den föreslagna lagens sekretessbestämmelser är sålunda till sin ordalydelse mera täckande än den allmänna offentlighetslagens.

De föreslagna bestämmelserna gäller handlingar som är sekretessbelagda i syfte att skydda en annan stats eller en internationell organisations viktiga allmänna intressen och som sålunda förutsätter en hög säkerhetsklassificering. Denna kategori av handlingar är i regel sekretessbelagd också enligt offentlighetslagens 24 § 1 mom. 2 punkten. Den största skillnaden är att en myndighet som beslutar om utlämnande av en handling enligt den internationella förpliktelsen om informationssäkerhet, skall motivera den skada som orsakas om informationen lämnas ut. I övrigt skall en informationsbegäran behandlas i enlighet med offentlighetslagen. Myndigheten skall sålunda säkerställa att klassificeringen av en handling motsvarar den som anges i överenskommelsen. Om det uppkommer oklarhet om huruvida klassificeringen är den rätta eller om vilken information i handlingen som föranleder klassificeringen, skall myndigheten kontakta den part som har upprättat handlingen. En sådan uttrycklig bestämmelse ingår i artikel 4.4. i överenskommelsen mellan Finland och Tyskland.

Ett syfte med den internationella regleringen av informationssäkerheten är att skapa ett system som gör det möjligt att skydda känslig information i situationer där en fördrags-

slutande stat ingår ett leveransavtal t.ex. om militärmateriel med ett företag i en annan stat och den information som utbyts i samband därmed berör viktiga nationella intressen och sålunda är i behov av skydd. Det land där företaget har hemvist fungerar i dessa situationer bl.a. som förmedlare av av säkerhetsklassificerat material. Om anbudsbegäran förmedlas till ett finländskt företag via en finsk myndighet innebär detta inte sådan offentlig maktutövning för vilken gäller bestämmelser om rätt till information i enlighet med offentlighetsprincipen.

Med stöd av det som anförs ovan kan den bedömningen göras att lagförslaget inte i sakligt hänseende minskar medborgarnas tillgång till information i förhållande till den rätt som de i detta avseende har enligt den gällande lagstiftningen.

Ett viktigt delområde i den föreslagna lagen är personsäkerheten. Den föreslagna lagen om internationella förpliktelser som gäller informationssäkerhet förutsätter att det förfarande som avses i lagen om säkerhetsutredningar används för att kontrollera anställdas tillförlitlighet. Den föreslagna lagen inskränker sålunda inte medborgarnas grundläggande rätt till personlig integritet och skydd för personuppgifter.

4.2. Verknningar för näringslivet

Genom de förslagna lagarna blir det möjligt för finländsk industri att delta i Europeiska rymdorganets projekt och framförallt i organisationens och Europeiska unionens gemensamma Galileoprogram. Om de internationella förpliktelserna som gäller informationssäkerhet inte fullgörs skulle detta avsevärt försämra den finländska industrins möjligheter att delta i det teknologiska utvecklingsarbetet och leveranserna. Om den finländska industrin inte får tillgång t.ex. till den klassificerade signalen för positionsbestämning (Public Regulated Signal, PRS) kommer dess konkurrensläge när det gäller utvecklingen av myndighetsinterna telefon-system sannolikt att försämrats, eftersom dessa med största sannolikhet kommer att ingå i det system som blir gemensamt för hela Europa.

4.3. Ekonomiska verkningar

Det är svårt att bedöma vilken betydelse de föreslagna bestämmelserna får för den finländska industrins konkurrensmöjligheter och för de finländska företagens deltagande i europeiska teknologiprojekt.

Storleksklassen av de ekonomiska verkningarna framgår emellertid av konstaterandet att Teknologiska utvecklingscentralen (Tekes) har investerat 7,3 miljoner euro i byggandet av de fyra första satelliterna och att enbart byggandet av de satelliter som är aktuella detta år betyder beställningar på ca 15 miljoner euro. De fyra första satelliterna som byggs i samarbete mellan europeiska industriföretag innebär leveranser på ca 1 000 miljoner euro. Den längsta effekten är emellertid av att den finländska telekommunikationsindustrin kan delta i sådana tillämpningar av mobil datakommunikation som utnyttjar Galileosignalerna. Det är då fråga om affärsverksamhet, t.ex. byggande av myndighetsradionät, som är värd hundratals miljoner eller rentav över en miljard euro.

Den föreslagna lagens ekonomiska verkningar inskränker sig emellertid inte till det europeiska rymdprogrammet och deltagandet i detta. I och med utvidgningen och förnyandet av de internationella avtalssystemen kommer lagstiftningen om företagens förpliktelser i fråga om informationssäkerheten att ge finländska företag bättre möjligheter att delta också i andra leveranser som innebär att företag bl.a. kan få tillgång till sekretessbelagd och klassificerad information.

Godkännandet av de överenskommelser och lagar som ingår i propositionen beräknas inte innebära några direkta betydande nya kostnader för förvaltningen. De internationella förpliktelserna om informationssäkerhet kommer uppenbarligen att medföra mera arbete, vilket innebär kostnader också för förvaltningen. Dessa kostnader behandlas närmare i avsnitt 4.4.

4.4. Administrativa effekter

Internationella överenskommelser om informationssäkerhet innehåller i regel bestämmelser om en nationell säkerhetsmyndighet (National Security Authority, NSA)

samt om utsedda säkerhetsmyndigheter (Designated Security Authority, DNS). Som exempel på sådana bestämmelser kan nämnas artikel 2 i säkerhetsskyddsavtalet mellan Finland och VEU samt vissa bestämmelser i den till avtalet anslutna säkerhetsstadgan.

Till den nationella säkerhetsmyndighetens uppgifter hör enligt de internationella överenskommelserna och andra förpliktelser i allmänhet att vidta arrangemang för skyddet av av säkerhetsklassificerad information samt för säkerhetsutredningar av personer och företag och utfärdande av säkerhetsintyg för personer som har tillgång till klassificerad information och som deltar i sådana möten och besök som definieras i förpliktelserna. Till den nationella säkerhetsmyndighetens uppgifter hör också att hålla kontakt med de fördragsslutande parterna och organisera besök samt att representera Finland i organ som behandlar informationssäkerhet.

I Finlands lagstiftning ingår för närvarande inga bestämmelser om en nationell säkerhetsmyndighet som sköter internationella förpliktelser gällande informationssäkerhet. I syfte att genomföra de internationella förpliktelserna om informationssäkerhet och öka det internationella förtroendet för Finlands förmåga att hantera känsligt material föreslås i propositionen att det förskrivs i lag om de myndigheter som skall sköta säkerhetsförpliktelserna. Det föreslås att uppgifterna som nationell säkerhetsmyndighet i detta skede skall skötas av utrikesministeriet, som redan nu sköter uppgifterna som nationell säkerhetsmyndighet i förhållande till Europeiska unionen samt VEU- och NATO-samarbetet. Försvarsministeriet, huvudstaben och skyddspolisen föreslås verka som utsedda säkerhetsmyndigheter. Dessa bestämmelser påverkar inte i något annat avseende uppgifterna eller befogenheterna för de myndigheter som behandlar säkerhetsärenden.

Den lösning som föreslås i propositionen är emellertid avsedd att vara temporär. Regeringen tillsätter våren 2004 ett beredningsorgan med uppgift att utreda hör det är mest ändamålsenlig att sköta den nationella säkerhetsmyndighetens uppgifter i Finland.

De internationella förpliktelserna som gäller informationssäkerhet kommer i varje fall att innebära nya uppgifter för huvudstaben,

som enligt den föreslagna lagen om internationella förpliktelser som gäller informationssäkerhet skall göra säkerhetsutredningar av företag. Resursbehoven bedöms närmare i samband med utredningen av hur den nationella säkerhetsmyndigheten skall organiseras med avseende på de internationella överenskommelserna om informationssäkerhet.

Avsikten är att i lagen om internationella förpliktelser som gäller informationssäkerhet ta in en bestämmelse enligt vilken beslutanderätten när det gäller sådana ansökningar om utlämnande av handlingar som avses i offentlighetslagen skall förbehållas den myndighet som i Finland verkar som mottagande myndighet. Detta kommer emellertid inte att ha någon större betydelse för förvaltningsverksamheten.

5. Ärendets beredning

På grund av att ärendet är brådskande har propositionen beretts som tjänsteuppdrag vid justitieministeriet. I beredningen har deltagit representanter för utrikesministeriet, försvarsministeriet, handels- och industriministeriet, finansministeriet, jord- och skogsbruksministeriet, huvudstaben, skyddspolisen och Teknologiska utvecklingscentralen (Tekes). Ministerierna, skyddspolisen och huvudstaben samt Industrin och arbetsgivarna r.f. har beretts tillfälle att framföra sin uppfattning om propositionsutkastet i olika skeden av beredningen. De synpunkter som framförts under förhandlingarna och av de sakkunniga som hörts har till väsentliga delar beaktats i propositionen.

6. Andra omständigheter som inverkat på propositionens innehåll

Så som framgår av statsrådets redogörelse om verkställighet av offentlighetslagstiftningen (SRR 5/2003 rd) är avsikten att ändra offentlighetslagen så att datasäkerheten kan utvecklas genom bestämmelser på lägre nivå. Utgående från försvarsministeriets framställning till justitieministeriet i mars 2004 utreds behovet att precisera offentlighetslagens bestämmelser om sekretesstiderna. I det sammanhanget kan det också göras en bedöm-

ning av behovet att justera bestämmelserna till följd av de internationella förpliktelserna om informationssäkerheten.

I propositionen föreslås att det stiftas en särskild lag om internationella förpliktelser som gäller informationssäkerhet. Lagen har ingen direkt betydelse för översynen av offentlighetslagen eller för utvecklandet av den

på denna baserade informationssäkerheten när det gäller nationellt informationsmaterial som myndigheterna har i sin besittning. Det finns inte något sådant direkt behov att se över bestämmelserna om sekretesstiderna att detta utgör något hinder för att godkänna de i denna proposition föreslagna lagarna före en eventuell översyn av offentlighetslagen.

DETALJMOTIVERING

1. Överenskommelsernas innehåll och förhållandet till Finlands lagstiftning

1.1. Överenskommelse mellan parterna i konventionen om upprättandet av Europeiska rymdorganet och Europeiska rymdorganet om skydd för och utbyte av av säkerhetsklassificerad information

Artikel 1. I artikeln definieras begreppet av säkerhetsklassificerad information. Överenskommelsen gäller information oberoende av vilken form den har. Frågan om hur informationen är registrerad saknar sålunda betydelse för tillämpningen av överenskommelsen. Finlands offentlighetslag har en motsvarande definition av begreppet handling (5 § 1 mom.).

Överenskommelsen omfattar endast material vars obehöriga röjande kan skada en eller flera fördragsslutande parter intressen och som har försetts med en säkerhetsklassificering.

Artikel 2. I denna artikel fastställs de fördragsslutande parternas viktigaste förpliktelser. Enligt artikelns första stycke gäller förpliktelserna för det första information som härstammar från ESA eller som överlämnas till ESA. Överenskommelsen gäller också information som producerats av en medlemsstat och som överlämnas till en annan medlemsstat till stöd för ett ESA-program, projekt eller -avtal.

Enligt artikelns andra stycke upprätthåller medlemsstaterna den säkerhetsklassificering av information som avses i avtalet och skyddar informationen i enlighet därmed. Enligt artikelns tredje stycke får informationen användas endast för de ändamål som anges i ESA-konventionen samt de beslut och resolutioner som hänför sig till konventionen. I artikelns fjärde stycke ingår ett förbud mot att avslöja sådan information som avses i överenskommelsen till stater som inte är parter i ESA-konventionen eller organ som lyder under deras jurisdiktion eller till någon annan internationell organisation, utan ett skriftligt

förhandsgodkännande av den som tillhandahåller informationen.

Enligt offentlighetslagen är traditionella diplomatiska handlingar samt handlingar som behandlas av statsrådets utrikes- och säkerhetspolitiska utskott i regel sekretessbelagda (24 § 2 mom. 1 punkten). Handlingar som gäller förhållandet mellan finska staten, finska medborgare, personer som vistas i Finland eller sammanslutningar som är verksamma i Finland och myndigheter, personer eller sammanslutningar i en främmande stat är sekretessbelagda, om utlämnande av uppgifter ur dem skulle medföra skada eller olägenhet för Finlands internationella förhållanden eller förutsättningar att delta i det internationella samarbetet (24 § 1 mom. 2 punkten). Bestämmelsen innebär i praktiken att en handling som en annan stat eller en internationell organisation har sänt till Finland och uttryckligen hänfört till någon av de högsta säkerhetsklasserna, anses vara sekretessbelagd också i Finland.

Eftersom den gällande lagstiftningen åtminstone enligt sin ordalydelse ger vederbörande myndighet prövningsrätt när det gäller omfattningen av sekretessbeläggningen, föreslås i lagförslaget en särskild sekretessbestämmelse om internationella krav på informationssäkerhet (lagförslag nr 3, 6 §).

Artikel 3. Denna artikel innehåller en bestämmelse om genomförande av ESA:s normer för dokumentssäkerhet för att säkerställa en enhetlig skyddsnivå för den klassificerade informationen. Inom ESA bereds en definition av de krav som anges i artikeln.

Artikel 4. Artikeln gäller säkerhetskontroll av personer. Syftet med förfarandet är att utreda om en person med avseende på hans eller hennes lojalitet och tillförlitlighet kan beviljas tillgång till av säkerhetsklassificerad information (tredje stycket). Varje fördragsslutande part samarbetar på begäran med andra fördragsslutande parter vid genomförandet av säkerhetsutredningar (fjärde stycket).

Enligt den första punkten i artikeln skall de stater som är fördragsslutande parter säkerställa att alla personer som på grund av sina

uppgifter behöver få tillgång till uppgifter eller material som har säkerhetsklassificerats, är vederbörligen säkerhetskontrollerade innan de beviljas tillgång till sådana uppgifter och sådant material. Enligt artikelns andra punkt skall de fördragsslutande parterna säkerställa att tillgång till sådan av säkerhetsklassificerad information som utbyts på basis av överenskommelsen beviljas endast personer som behöver uppgifterna för utförande av sina uppgifter.

I Finland säkerhetskontrolleras personer på det sätt som föreskrivs i lagen om säkerhetsutredningar. Dessa bestämmelser behöver inte ändras till följd av artikeln.

Artikel 5. Enligt artikeln skall det säkerställas att överenskommelsens bestämmelser verkställs inom ESA.

Artikel 6. Enligt denna artikel skall de fördragsslutande parterna undersöka alla fall där det konstateras eller misstänks att av säkerhetsklassificerad information som har lämnats eller producerats inom ramen för denna överenskommelse har äventyrats eller förlorats (punkt 1). Varje fördragsslutande part informerar vid behov snabbt och grundligt andra fördragsslutande parter om alla detaljer som ansluter sig till fallet och om eventuella resultat av undersökningen samt om alla åtgärder som har vidtagits för att förhindra en upprepning av dylikt röjande av information.

I Finlands lagstiftning finns inga särskilda bestämmelser om utredningsskyldighet vid misstanke om brott mot sekretess- eller säkerhetsbestämmelser och inte heller bestämmelser som innebär att den måste underrättas vars information har röjts. Avsikten är att ta in bestämmelser om saken i den föreslagna lagen om internationella förpliktelser som gäller informationssäkerhet (lagförslag nr 3, 18 §).

Artikel 7. Artikeln gäller en medlemsstats, ESA:s råds och generaldirektörens skyldighet att i enlighet med ESA-konventionen avstå från sin immunitet då en representant för en medlemsstat, ESA:s generaldirektör eller en medlem av ESA:s personal eller någon av dess experter är part i en rättsprocess som gäller obehörigt röjande av av säkerhetsklassificerad information.

Artikel 8. I denna artikel konstateras att överenskommelsen inte på något sätt hindrar

att de fördragsslutande parterna vidtar andra arrangemang i anslutning till utbyte av sådan av säkerhetsklassificerad information som härstammar från dem och som inte påverkar tillämpningsområdet för denna överenskommelse.

Artikel 9. Denna artikel gäller ändring av överenskommelsen. Varje fördragsslutande part kan föreslå ändringar i överenskommelsen. Varje ändring av överenskommelsen träder i kraft trettio dagar efter det att Frankrikes regering har mottagit ett meddelande om godkännande från alla fördragsslutande parter. Frankrikes regering informerar alla fördragsslutande parter om datumet för ikraftträdande av varje ändring.

Artikel 10. Denna artikel innehåller bestämmelser om undertecknande, godkännande och ikraftträdande av överenskommelsen. Ratifikations-, godtagande- eller godkännandeinstrumenten skall deponeras hos Frankrikes regering. Överenskommelsen träder i kraft trettio dagar efter det att två signatärstater har deponerat sina ratifikations-, godtagande- eller godkännandeinstrument. I förhållande till varje annan signatärstat träder överenskommelsen i kraft trettio dagar efter det att den staten har deponerat sitt ratifikations-, godtagande- eller godkännandeinstrument.

Artikel 11. I denna artikel regleras nya parter tillträdande av överenskommelsen. Artikeln behandlar inte frågor som hör till lagstiftningens område.

Artikel 12. I denna artikel ingår bestämmelser om uppsägning av överenskommelsen. Överenskommelsen får sägas upp genom en skriftlig underrättelse om uppsägning till depositarien. Uppsägningen träder i kraft ett år efter det att depositarien har mottagit underrättelsen.

Enligt artikelns andra stycke påverkar uppsägningen inte en fördragsslutande parts skyldighet att skydda och bevara den av säkerhetsklassificerade information som parten har fått tillgång till inom ramen för denna överenskommelse. Detsamma gäller också i det fall att en fördragsslutande part säger upp ESA-konventionen eller i det fall att Europeiska rymdorganet upphör att existera i enlighet med konventionen.

Artikeln andra punkt förutsätter reglering

på lagnivå och har därför beaktats i den föreslagna lagen om internationella förpliktelser som gäller informationssäkerhet (lagförslag nr 3, 15 §).

Artikel 13. Denna artikel gäller depositariens underrättelser om deposition av ratifikations-, godtagande- och godkännande- eller uppsägningsinstrument.

1.2. Överenskommelse mellan Finland och Tyskland om ömsesidigt skydd för av säkerhetsklassificerad information

Artikel 1. Syfte. Enligt denna artikel är syftet med överenskommelsen att skydda av säkerhetsklassificerad information som utbyts mellan Finland och Tyskland. Den allmänna skyddsförpliktelsen uttrycks i överenskommelsens artikel 5.1 enligt vilken de fördragsslutande parterna förbinder sig att tillförsäkra den andra fördragsslutande partens information minst samma skydd som den ger åt sin egen information som hör till samma säkerhetsklass.

I artikel 1 nämns de funktioner som överenskommelsen tillämpas på. Tillämpningsområdet kan indelas i två delar: för det första i informationsutbyte inom samarbetet mellan de avtalsparter som räknas upp i artikeln samt för det andra i sådana överenskommelser mellan den andra fördragsslutande partens myndigheter och den andra fördragsslutande partens företag som i överenskommelsen benämns av säkerhetsklassificerade avtal.

Överenskommelsen tillämpas på utbyte av av säkerhetsklassificerad information som har samband med de internationella relationerna, försvaret, polis- eller industriärenden. Det är skäl att observera att avtalet inte gäller vilken som helst information i samband med de funktioner som räknas upp i artikeln utan endast information som uttryckligen har av säkerhetsklassificerats i den andra fördragsslutande staten. Det är sålunda fråga om känsligt information som äventyrar nationella intressen.

Överenskommelsen tillämpas inte enbart på relationerna mellan myndigheter. Den tillämpas också i samband med avtal som en enhet inom en fördragsslutande parts offentliga förvaltning har ingått med en privat eller

offentlig inrättning i en annan fördragsslutande stat.

Artikel 2. Definitioner. I denna artikel definieras den information som omfattas av överenskommelsen. Med information avses fakta, uppgifter eller underrättelser som oavsett formen skall beläggas med sekretess i allmänintressets namn. Klassificeringen av informationen skall göras av en behörig myndighet eller av någon som verkar på uppdrag av denna, alltefter behovet av skydd.

Sekretessplikten omfattar både dokumentsekretess och tystnadsplikt, dvs. skyldigheten att hemlighålla information. De definitioner som används i Tyskland respektive i Finland överensstämmer sinsemellan, utom i det avseendet att i den definition som tillämpas i Finland dessutom nämns att sekretessplikten är baserad på lag. Detta beror på att grundlagens 12 § 2 mom. föreskriver att offentligheten när det gäller myndigheters handlingar kan begränsas endast genom lag.

Artikel 3. Överensstämmelse. I denna artikel definieras säkerhetsklasserna samt fastställs överensstämmelsen mellan Tysklands och Finlands säkerhetsklasser. I offentlighetsförordningen anges de finländska säkerhetsklasserna för nationella dokument. Överenskommelsens definitioner skiljer sig delvis från de nationella definitionerna, på grund av att endast allmänna intressen kommer i fråga som skyddsobjekt enligt överenskommelsen.

Enligt överenskommelsen är säkerhetsklasserna fyra till antalet och de definieras enligt hur allvarligt ett obehörigt röjande av informationen anses vara med tanke på de skyddade intressena.

Den högsta klassen som kräver stränga åtgärder när det gäller informationssäkerheten är "ytterst hemlig" (STRENG GEHEIM). Till denna klass räknas i Finland information vars obehöriga röjande kan orsaka särskilt påtaglig skada för försvaret, säkerheten, de internationella relationerna eller andra allmänna intressen. Finlands internationella relationer skyddas i enlighet med offentlighetslagens 24 § 1 mom. 1 och 2 punkten, försvarets intressen i paragrafens 1 mom. 10 punkten och säkerheten i paragrafens 1 mom. 5, 8 och 9 punkten. Andra allmänna intressen som avses i definitionen är t.ex. skyddsarrangemang för statsledningen och statsbesök

samt för datasystem (24 § 1 mom. 7 punkten) samt samhällsekonomin (24 § 1 mom. 11 och 12 punkten).

Den andra säkerhetsklassen är ”hemlig” (GEHEIM) till denna kategori hör information vars obehöriga röjande kan orsaka väsentlig skada för försvaret, säkerheten, de internationella relationerna eller andra allmänna intressen.

Den tredje säkerhetsklassen är ”konfidentiell” (VS-VERTRAULICH) varmed avses information vars obehöriga röjande kan skada försvaret, säkerheten, de internationella relationerna eller andra allmänna intressen.

På information som hör till den fjärde klassen ”begränsad tillgång” (VS-NUR FÜR DEN DIENSTGEBRAUCH) tillämpas endast en del av de förpliktelser som anges i överenskommelsen. Till denna klass hör information vars obehöriga röjande kan skada det allmänna intresset eller begränsa myndigheternas möjligheter att agera.

Artikel 4. Märkning. Enligt denna artikel skall den sändande fördragsslutande staten förse klassificerad information med en säkerhetsklassificering som motsvarar den mottagande statens nationella klassificering. Denna märkningsskyldighet gäller enligt artikelns andra stycke också sådan information som i den mottagande staten har producerats på basis av den information som förmedlats av den andra fördragsslutande staten.

Enligt artikelns tredje stycke skall säkerhetsklassificeringen upphävas om den behöriga myndigheten i ursprungslandet begär det. Den andra fördragsslutande statens behöriga myndighet skall på förhand underrätta den behöriga myndigheten i ursprungslandet om sin avsikt.

Enligt artikelns fjärde stycke kan den behöriga myndigheten i det land som mottagit av säkerhetsklassificerad information be den behöriga myndigheten i ursprungslandet att ändra klassificeringen eller be den ge en motivering till valet av viss säkerhetsklass.

Enligt Finlands lagstiftning gäller inte någon sådan av säkerhetsklassificeringsskyldighet som avses i överenskommelsen. Därför föreslås att bestämmelser om saken tas in i lagen om internationella förpliktelser som gäller informationssäkerhet (lagförslag nr 3, 8 §). Artikelns fjärde stycke skall beaktas då

en finsk myndighet ombes lämna ut uppgifter om en av säkerhetsklassificerad handling. Myndigheten skall enligt offentlighetslagens 17 § se till att möjligheterna att få information inte begränsas mer än vad som är nödvändigt för det intresse som skall skyddas. Om det t.ex. på grund av att en längre tid har förflutit inte längre förefaller finnas några grunder för en säkerhetsklassificering, skall myndigheten kontakta den tyska myndighet som har fastställt säkerhetsklassen.

Artikel 5. Åtgärder på den nationella nivån. Artikelns första stycke innehåller överenskommelsens centrala princip enligt vilken de fördragsslutande parterna förbinder sig att vidta alla nödvändiga åtgärder för att skydda sådan av säkerhetsklassificerad information som har förmedlats på basis av överenskommelsen eller producerats i anslutning till ett av säkerhetsklassificerat avtal. De skall försäkra informationen i fråga minst samma skydd som de ger åt sin egen information som hör till samma nationella säkerhetsklass.

Såsom framgår ovan är det inte obligatoriskt att i Finland av säkerhetsklassificera handlingar enligt krav på sekretess och informationssäkerhet. Därför föreslås att i lagen om internationella förpliktelser som gäller informationssäkerhet tas in bestämmelser om obligatorisk klassificering (lagförslag nr 3, 8 §).

Artikelns andra stycke gäller information som hör till den lägsta säkerhetsklassen (”begränsad tillgång”). Endast en del av överenskommelsens mera detaljerade bestämmelser gäller denna kategori av information. Enligt huvudregeln skall information som hör till denna klass behandlas på samma sätt som information som hör till motsvarande klass i den mottagande staten.

Enligt artikelns tredje stycke får de fördragsslutande parterna inte röja den av säkerhetsklassificerade information som de mottagit för internationella organisationer eller för någon tjänsteman eller person i tredje land utan att den behöriga myndighet som fattat av klassificeringsbeslutet har gett sitt samtycke. Den klassificerade informationen får användas endast för angivet ändamål. Tillgång till av säkerhetsklassificerad information får beviljas endast personer som behöver ha tillgång till uppgifterna för skötsel

av sina uppgifter.

Enligt finländsk lag är sekretessbeläggningen av en handling som en annan stat har sänt till en finsk myndighet beroende av vilka följder utlämnandet av handlingen skulle ha. Av denna anledning föreslås att i lagen om internationella förpliktelser som gäller informationssäkerhet tas in en specialbestämmelse om sekretessplikt (lagförslag nr 3, 6 §).

Artikel 6. Säkerhetsklassificerade avtal. Denna artikel innehåller bestämmelser med tanke på situationer där ett företag inom en fördragsslutande stats territorium har ingått eller har för avsikt att ingå ett sådant avtal med en myndighet eller ett företag i en annan fördragsslutande stat, som innebär att uppdragstagaren eller dess personal får tillgång till av säkerhetsklassificerad information (första stycket).

Enligt artikelns andra stycke skall uppdragsgivaren innan ett avtal som tillhör säkerhetsklassen VS-VERTRAULICH / KONFIDENTIELL eller en högre säkerhetsklass ingås, genom sin egen behöriga myndighet få en säkerhetsutredning som gäller uppdragstagaren (säkerhetsutredning som gäller sammanslutning). Genom denna utredning säkerställs det att en eventuell avtalspart – t.ex. ett företag som deltar i leveranser till Tysklands försvarsmakt eller en underleverantör till ett tyskt företag – är föremål för säkerhetsövervakning av sitt eget lands behöriga myndighet samt att avtalsparten har vidtagit nödvändiga säkerhetsåtgärder. I artikelns andra stycke, punkterna 1–7, finns närmare bestämmelser om förfarandet.

I Finlands lagstiftning finns för närvarande inga bestämmelser om av säkerhetsklassificerade avtal och inte heller några bestämmelser om säkerhetsutredningar som gäller företag. Avsikten är att ta in bestämmelser om saken i den föreslagna lagen om internationella förpliktelser som gäller informationssäkerhet (lagförslag nr 3, i synnerhet 1 § 2 mom., 2 § 2 punkten, 7 § samt 12 och 13 §).

Enligt artikelns tredje stycke skall de fördragsslutande parterna vidta alla nödvändiga åtgärder för att säkerställa att av säkerhetsklassificerade avtal innehåller en klausul som ålägger uppdragstagaren att vidta nödvändiga åtgärder för att skydda av säkerhetsklassifi-

cerad information i enlighet med det egna landets nationella säkerhetsbestämmelser. Bestämmelser om detta föreslås i 13 § i lagen om internationella förpliktelser som gäller informationssäkerhet.

Enligt artikelns fjärde stycke skall uppdragsgivarens behöriga myndighet ge uppdragstagaren en särskild förteckning (klassifikationsguide) över alla dokument som kräver klassificering. Den behöriga myndigheten skall också bestämma vilken säkerhetsklass som skall gälla och se till att förteckningen bifogas till av säkerhetsklassificerade avtal. Uppdragsgivarens behöriga myndighet skall vidarebefordra förteckningen eller se till att den vidarebefordras till uppdragstagarens behöriga myndighet.

Enligt artikelns femte stycke skall uppdragsgivarens behöriga myndighet säkerställa att uppdragstagaren ges tillgång till av säkerhetsklassificerad information först efter det att uppdragstagarens behöriga myndighet har lämnat den nödvändiga säkerhetsutredningen som gäller sammanslutning.

Artikel 7. Förmedling av av säkerhetsklassificerad information. I artikeln ingår detaljerade bestämmelser om förfarandet vid förmedling av säkerhetsklassificerad information.

Artikel 8. Besök. Artikeln innehåller bestämmelser om förfarandet då för representanterna för en fördragsslutande part ordnas tillfälle att bekanta sig med en annan fördragsslutande parts skötsel av sina uppgifter i samband med informations säkerheten.

Artikel 9. Förhandlingar. I denna artikel föreskrivs om förfarandet i situationer där en avtalspart vill förhandla i ett ärende som gäller tillämpning av överenskommelsen.

Artikel 10. Brott mot bestämmelserna om ömsesidigt skydd av säkerhetsklassificerad information. Enligt denna artikel skall en fördragsslutande part underrättas om obehörigt röjande av klassificerad information misstänks eller har konstaterats.

I Finlands lagstiftning finns inga bestämmelser som förpliktar myndigheterna att underrätta myndigheterna i en annan stat om konstaterade lagstridiga förfaranden. I den föreslagna lagen om internationella förpliktelser som gäller informationssäkerhet tas in uttryckliga bestämmelser om saken (lagför-

slag nr 3, 19 §).

Enligt artikelns andra punkt skall alla ärenden som gäller brott mot bestämmelserna om skydd av säkerhetsklassificerad information undersökas och relevanta åtgärder vidtas. Den andra fördragsslutande parten skall på begäran bistå vid undersökningen och bli informerad om resultatet av den.

Artikel 11. Kostnader. Vardera fördragsslutande parten skall svara för de kostnader som orsakas av de behöriga myndigheternas verksamhet.

Artikel 12. Behöriga myndigheter. I denna artikel föreskrivs om skyldigheten att underätta den andra fördragsslutande parten om vilka myndigheter som är behöriga när det gäller verkställigheten av överenskommelsen.

Artikel 13. Slutbestämmelser. I denna artikel föreskrivs om överenskommelsens ikraftträdande samt om ändring, uppsägning och registrering av överenskommelsen. Överenskommelsen träder i kraft femton dagar efter att Tyskland har mottagit ett meddelande från Finland om att de nationella åtgärder som behövs för överenskommelsen ikraftträdande har vidtagits.

När överenskommelsen träder i kraft upphör det dokument av den 22 december 1997 som inbegriper en överenskommelse mellan republiken Finlands försvarsministerium och Tyska förbundsrepublikens försvarsministerium om ömsesidigt skydd för sekretessbelagd försvarsinformation att gälla. På material som har överlämnats med stöd av dokumentet skall den nya överenskommelsen tillämpas.

2. Motivering av lagförslagen

2.1. Lag om sättande i kraft av de bestämmelser som hör till området för lagstiftningen i överenskommelsen mellan parterna i konventionen om upprättandet av Europeiska rymdorganet och Europeiska rymdorganet om skydd för och utbyte av säkerhetsklassificerad information

Enligt grundlagens 95 § skall de bestämmelser i internationella förpliktelser som hör till området för lagstiftningen sättas i kraft

nationellt genom en särskild lag om saken. De bestämmelser i en internationell förpliktelse som hör till området för lagstiftningen skall sättas i kraft genom en blankettlag eller en blandlag också i det fall att förpliktelsen leder till att det materiella innehållet i den nationella lagstiftningen måste revideras. Propositionen innehåller ett förslag till en blankettlag.

1 §. Genom den föreslagna lagens 1 § sätts de bestämmelser i överenskommelsen i kraft som hör till området för lagstiftningen. De bestämmelser som hör till området för lagstiftningen refereras nedan i avsnittet om behovet av riksdagens samtycke.

2 §. Föreskrifter om lagens ikraftträdande utfärdas genom förordning av republikens president. Avsikten är att lagen skall träda i kraft samtidigt som överenskommelsen träder i kraft för Finlands del.

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

I fråga om detta lagförslag kan anföras samma som ovan i det inledande stycket i avsnitt 2.1. Propositionen innehåller ett förslag till en blankettlag.

1 §. Genom den föreslagna lagens 1 § sätts de bestämmelser i överenskommelsen i kraft som hör till området för lagstiftningen. De bestämmelser som hör till området för lagstiftningen refereras nedan i avsnittet om behovet av riksdagens samtycke.

2 §. Föreskrifter om lagens ikraftträdande utfärdas genom förordning av republikens president. Avsikten är att lagen skall träda i kraft samtidigt som överenskommelsen träder i kraft för Finlands del.

2.3. Lag om internationella förpliktelser som gäller informations säkerhet

1 kap. Allmänna bestämmelser

1 §. *Lagens tillämpningsområde.* I denna paragraf anges vad som regleras i den föreslagna lagen. Tillämpningsområdet täcker de

två situationer som det föreskrivs om i paragrafens 1 och 2 mom.

Enligt den föreslagna paragrafens 1 mom. föreskrivs i lagen om myndigheternas åtgärder vid fullgörandet av internationella förpliktelser som gäller informationssäkerhet. I lagförslagets 2 § definieras begreppet internationell förpliktelse som gäller informationssäkerhet. Det är huvudsakligen myndigheterna som skall fullgöra dessa förpliktelser. I lagen definieras inte begreppet myndighet. I lagförslagets 3 § hänvisas till offentlighetslagens definition av begreppet myndighet.

Lagen skall enligt paragrafens 2 mom. tillämpas också på näringsidkare och dessas anställda då en näringsidkare är part i ett säkerhetsklassificerat avtal eller deltar i ett upphandlingsförfarande innan ett sådant avtal sluts eller är underleverantör till en sådan näringsidkare. Med näringsidkare avses en sammanslutning eller fysisk person som bedriver näringsverksamhet. I lagförslagets 2 § 3 mom. definieras begreppet säkerhetsklassificerat avtal.

Lagens 12–14 § samt 16 § 2 mom. skall enligt den föreslagna paragrafens 3 mom. tillämpas också på näringsidkare som ber om en säkerhetsutredning och bedömning för att kunna delta i ett anbudsförfarande som ordnas av en myndighet i en annan stat eller av ett företag som har hemvist i den andra staten. Syftet med bestämmelsen är att trygga finländska företags möjligheter att konkurrera om leveranser också i sådana fall då det inte finns något internationellt avtal om informationssäkerhet som kan tillämpas på leveransen. Det är fråga om leveranser för vilka myndigheterna i den andra staten förutsätter att de som deltar i anbudsförfarandet och avtalsparterna skall vara särskilt tillförlitliga. Enligt lagförslagets 12 § kan sådan säkerhetsutredning och bedömning som gäller sammanslutning göras på begäran av en näringsidkare oberoende av internationella överenskommelser.

I lagförslagets 2 § ingår bestämmelser som är centrala när det gäller det materiella tillämpningsområdet för lagen. Med beaktande av dessa bestämmelser kan det konstateras att den föreslagna lagen skall tillämpas för det första på sekretessbelagda handlingar och informationsmaterial som har tillställts

en finsk myndighet, då avsändaren i enlighet med en internationell överenskommelse som är bindande för Finland eller någon annan förpliktelse har försett försändelsen med en säkerhetsklassificering. Lagens tillämpningsområde omfattar för det andra en av en finsk myndighet eller av en till lagens tillämpningsområde hörande näringsidkare upprättad handling varav framgår information som ingår i en handling som har sänts till Finland eller information som kan hämtas ur ett visst material. Lagens tillämpningsområde omfattar likaså handlingar och material som har producerats i Finland inom ramen för säkerhetsklassificerad information.

2 §. *Definitioner.* I denna paragraf definieras begreppen internationell förpliktelse som gäller informationssäkerhet, särskilt känsligt informationsmaterial samt klassificerat avtal.

Enligt 1 punkten i den föreslagna paragrafen avses med en internationell förpliktelse som gäller informationssäkerhet en bestämmelse som ingår i en antingen multi- eller bilateral internationell överenskommelse som är bindande för Finland samt en sådan annan för Finland bindande författning som gäller åtgärder för skydd av särskilt känsligt material.

De överenskommelser som avses i lagen är för det första den överenskommelse som den 19 augusti 2002 ingicks mellan parterna i konventionen om upprättandet av Europeiska rymdorganet och Europeiska rymdorganet om skydd för och utbyte av säkerhetsklassificerad information. I propositionen föreslås att denna överenskommelse godkänns och sätts i kraft. Den andra överenskommelsen är den överenskommelse som den 25 februari 2004 ingicks mellan republiken Finland och Tyska förbundsrepubliken om ömsesidigt skydd för säkerhetsklassificerad information. I propositionen föreslås att också denna godkänns och sätts i kraft. Bland de övriga fördrag som avses i den föreslagna lagen kan nämnas säkerhetsskyddsavtalet mellan Finland och Västeuropeiska unionen. Förslaget innebär att en internationell överenskommelse i framtiden skall godkännas och sättas i kraft på det sätt som föreskrivs i grundlagen för att den skall höra till lagens tillämpningsområde.

Med en annan författning som är bindande

för Finland avses en sådan internationell författning som är bindande för Finland utan att det behövs någon särskild författning, t.ex. en EG-förordning, som sätter den i kraft. En för Finland bindande författning av det slag som avses i denna punkt är EU-rådets beslut om antagande av rådets säkerhetsbestämmelser 2001/264/EG, som förutsätter att medlemsstaterna vidtar nationella åtgärder för att bestämmelserna i beslutet skall kunna respekteras.

Med ett särskilt känsligt informationsmaterial avses i 2 punkten sådana sekretessbelagda handlingar och material samt information som kan fås ur dem som enligt en internationell förpliktelse om informationssäkerhet har säkerhetsklassificerats. Särskilt känsligt informationsmaterial är sålunda handlingar som har tillställts en finsk myndighet samt i handlingarna ingående information som den ena fördragsslutande parten har säkerhetsklassificerat i enlighet med överenskommelsen. Detsamma gäller sekretessbelagt material varmed avses anordningar och andra föremål som, om de undersöks, avslöjar eller kan avslöja sekretessbelagda omständigheter, t.ex. information som äventyrar försvaret eller säkerheten. Särskilt känsligt informationsmaterial är enligt definitionen också sådana av en finsk myndighet upprättade handlingar som innehåller säkerhetsklassificerad information som en annan fördragsslutande part har sänt till Finland och likaså handlingar och material som har producerats inom ramen för särskilt känsligt informationsmaterial.

Med ett säkerhetsklassificerat avtal avses enligt paragrafens 3 punkt 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 anbudsgivning eller fullgörande av ett avtal kan förutsätta tillgång till särskilt känsligt informationsmaterial.

Lagen skall enligt förslaget inte tillämpas på vilka som helst handlingar som har samband med internationellt samarbete utan en-

dast på handlingar som berör någon internationell förpliktelse om informationssäkerhet. Sådana förpliktelser avser endast handlingar som är sekretessbelagda i den sändande staten eller i en internationell organisation eller i ett internationellt organ och, även av dessa, endast sådana handlingar som hör till särskilda säkerhetsklasser.

Som definition av begreppet handling skall i enlighet med hänvisningsbestämmelsen i den föreslagna lagens 3 § tillämpas offentlighetslagens 5 § 1 mom. Med handling avses sålunda utöver traditionella handlingar också elektroniska och andra upptagningar som kan avläsas endast med tekniska hjälpmedel.

3 §. *Förhållande till annan lagstiftning.* I paragrafen anges den föreslagna lagens förhållande till andra bestämmelser som gäller informationssäkerhet för myndigheters handlingar. Enligt 1 mom. är huvudregeln den att i fråga om offentligheten för särskilt känsligt informationsmaterial samt i fråga om en god informationshantering i samband med sådant material gäller vad som föreskrivs i och med stöd av offentlighetslagen, om inte något annat föreskrivs i den föreslagna lagen. Sålunda tillämpas i detta sammanhang t.ex. den definition av begreppet handling som ingår i offentlighetslagens 5 § 1 mom.

I den föreslagna lagen ingår flera bestämmelser som helt avviker från tidigare bestämmelser om informationssäkerhet för handlingar. Det oaktat är det viktigt att ta in en allmän hänvisningsbestämmelse i offentlighetslagen. Till de delar som det i finska myndigheters handlingar ingår annan information än sådan som avses i internationella förpliktelser om informationssäkerhet, skall offentlighetslagen och bestämmelser som har utfärdats med stöd av den tillämpas. Med dessa kan jämföras också anvisningarna om tillämpning av bestämmelserna, i synnerhet om de krav på informationssäkerhet som motsvarar de olika säkerhetsklasserna.

Det bör observeras att handlingsoffentligheten kan påverkas också av någon annan författning som är bindande för Finland. I fråga om handlingar på vilka tillämpas Europaparlamentets och rådets förordning (EG) nr 1049/2001 om allmänhetens tillgång till Europaparlamentets, rådets och kommissionens handlingar, gäller vad som föreskrivs i den

nämnda författningen. Sekretessplikten i fråga om känsliga handlingar som sänds från EU till Finland skall således bedömas i enlighet med artikel 9.5 i den nämnda förordningen.

I paragrafens 2 *mom.* har tagits in en specialbestämmelse om beslutanderätten i en situation där information med stöd av offentlighetslagen begärs om sådant särskilt känsligt material som avses i lagförslaget.

Enligt offentlighetslagen kan en begäran om information behandlas och avgöras av den myndighet som innehar handlingen. En begäran om att få ta del av en handling kan emellertid överföras till en annan myndighet i sådana situationer som avses i offentlighetslagens 15 §.

Enligt förslaget skall en på lagen om offentlighet i myndigheternas verksamhet eller på någon annan lag baserad begäran om att få tillgång till särskilt känsligt informationsmaterial behandlas av den myndighet som informationsmaterialet har sänts till eller som ärendet skall behandlas av i sin helhet. Syftet med bestämmelsen är att centralisera behandlingen och avgörandet av ärenden som gäller särskilt känsligt informationsmaterial till den myndighet som har de bästa förutsättningarna att sköta ärendet.

Även om särskilt känsligt material är sekretessbelagt finns det i vissa situationer, t.ex. på grund av att en lång tid har förflutit, inte nödvändigtvis något behov av att hålla hela materialet hemligt. I sådana situationer skall myndigheten se till att den andra stat eller den internationella organisation eller det internationella organ som har sänt informationsmaterialet till Finland kontaktas för en översyn av säkerhetsklassificeringen. Också denna bedömning lämpar sig bäst för den myndighet som skall sköta hela ärendet inom ramen för den internationella förpliktelsen om informationssäkerhet.

2 kap. **Säkerhetsmyndigheterna och samarbetet mellan dem**

4 §. *Den nationella säkerhetsmyndigheten och de utsedda säkerhetsmyndigheterna.* I denna paragraf föreskrivs om de myndigheter som svarar för att de internationella förpliktelserna om informationssäkerhet fullgörs.

Enligt 1 *mom.* i den föreslagna paragrafen skall utrikesministeriet verka som nationell säkerhetsmyndighet (National Security Authority, NSA) i ärenden som gäller internationella förpliktelser om informationssäkerhet. Utrikesministeriet sköter redan för närvarande uppgifterna som nationell säkerhetsmyndighet när det gäller Europeiska unionens, NATO:s samt Västeuropeiska unionens verksamhet. Till den nationella säkerhetsmyndighetens uppgifter hör enligt de internationella överenskommelserna att svara för dokumentssäkerheten i sådana fall som avses i överenskommelserna, att svara för kontrollen av säkerhetsarrangemang samt att säkerställa att de anställda vid nationella myndigheter som har tillgång till säkerhetsklassificerad information har varit föremål för säkerhetsutredning samt att deras tillförlitlighet har bedömts på basis av utredningen.

Försvarsministeriet, huvudstaben och skyddspolisen skall enligt förslaget verka som utsedda säkerhetsmyndigheter (Designated Security Authority, DSA). Dessa myndigheter skall t.ex. enligt det säkerhets- skyddsavtal som har ingåtts med VEU bl.a. svara för säkerhetsklassificeringen av handlingar i anslutning till anbuds- och leveransförfaranden.

Enligt lagen om säkerhetsutredningar är det i Finland skyddspolisen och huvudstaben som svarar för utredningar som gäller personsäkerhet. I lagförslagets 11 § föreslås bestämmelser om sådana säkerhetsutredningar. Vid säkerhetsutredningar som gäller personer skall i huvudsak iaktas den nuvarande behörighetsfördelningen. Säkerhetsutredningar som gäller sammanslutningar skall däremot i detta skede, enligt lagförslagets 12 § göras av huvudstaben, som har erfarenhet på området.

I paragrafens 2 *mom.* föreslås en bestämmelse som berättigar statsrådet att genom förordning utfärda föreskrifter om uppgiftsfördelningen mellan säkerhetsmyndigheterna.

Såsom konstateras i den allmänna motiveringen skall regeringen särskilt reda ut hur det är ändamålsenligast att permanent ordna skötseln av uppgifter som ingår i de internationella förpliktelserna om informationssäkerhet. På grund av den snabba utvecklingen inom området och bl.a. med tanke på utveck-

lingen av den finländska teknologiska kompetensen är det emellertid skäl att redan i detta skede bygga upp arrangemang som tryggar Finlands och den finländska industrins möjligheter att delta i det internationella samarbetet. De internationella bestämmelserna påverkar inte i något annat avseende de myndigheters befogenheter som sköter säkerhetsärenden.

5 §. *Informationsutbyte och samarbete mellan säkerhetsmyndigheterna.* Enligt paragrafens 1 mom. skall säkerhetsmyndigheterna samarbeta för att på ett ändamålsenligt sätt uppfylla internationella förpliktelserna som gäller informationssäkerhet samt i detta syfte utbyta information, utan hinder av vad som föreskrivs om sekretessplikten.

I paragrafens 2 mom. föreslås bestämmelser som gör det möjligt att sköta uppgifterna på ett så ändamålsenligt sätt som möjligt. Enligt förslaget kan säkerhetsmyndigheterna komma överens om att en säkerhetsmyndighet sköter en viss uppgift eller ett visst uppgiftsområde för den andra säkerhetsmyndighetens räkning, om arrangemanget behövs för att uppgifterna skall kunna skötas på ett ändamålsenligt, ekonomiskt och flexibelt sätt.

3 kap. Åtgärder som gäller informationssäkerheten

6 §. *Sekretess och användning av information.* I denna paragraf föreskrivs om särskilt känsligt informationsmaterial samt om användning av information.

Enligt paragrafens 1 mom. skall särskilt känsligt informationsmaterial sekretessbeläggas. Ett syfte med totalrevideringen av offentlighetslagen (RP 30/1998 rd) var att sammanställa alla sekretessbestämmelser om myndighetshandlingar i offentlighetslagen. I sitt svar på regeringens proposition med förslag till totalrevidering av offentlighetslagstiftningen förutsatte riksdagen att regeringen iakttar restriktivitet när det gäller att ta in bestämmelser om sekretess för myndighetsuppgifter i speciallagstiftning (RSv 303/1998 rd).

Såsom ovan konstateras gäller de internationella förpliktelserna om informationssäkerhet i vissa situationer också näringsidkare. Av denna anledning är det skäl att i lagför-

slaget föreskriva också om näringsidkares sekretessplikt när det gäller handlingar. Det är skäl att utforma bestämmelsen så att den innebär ovillkorlig sekretessplikt. Om denna specialbestämmelse inte skulle gälla myndigheter skulle detta betyda att för samma material gäller två bestämmelser som är utformade på olika sätt, trots att vardera syftar till samma slutresultat.

Lagförslaget innebär att en handling skall sekretessbeläggas om den har producerats i Finland på det sätt som avses i en internationell förpliktelse om informationssäkerhet och om den har säkerhetsklassificerats av producenten i enlighet med en överenskommelse eller författning. En handling som har upprättats av en finsk myndighet för samarbete av det slag som avses i överenskommelsen och som innehåller sekretessbelagd och säkerhetsklassificerad information som har producerats i Finland skall enligt förslaget sekretessbeläggas. Till övriga delar skall offentlighetslagen tillämpas på en handling av det sist nämnda slaget.

Enligt paragrafens 2 mom. får särskilt känsligt informationsmaterial användas och överlåtas endast för angivet ändamål, om inte den som säkerhetsklassificerat materialet har samtyckt till något annat. Användningen av särskilt känsligt informationsmaterial är sålunda starkt ändamålsbunden. I internationella överenskommelser som gäller utbyte av sekretessbelagd information mellan olika länders myndigheter ingår i regel en bestämmelse som begränsar användningen av informationen.

En myndighet som hanterar särskilt känsligt informationsmaterial skall enligt paragrafens 3 mom. se till att endast sådana personer har tillgång till informationsmaterialet som behöver informationen för skötsel av sina uppgifter. Dessa personer skall i sådana fall som avses i förpliktelsen namnges på förhand. Detsamma gäller näringsidkare som avses i 1 § 2 mom.

I förslaget har skrivits in det i internationella överenskommelser allmänna kravet att en myndighet internt skall iaktta stor restriktivitet vid användningen av säkerhetsklassificerad information och att endast sådana personer skall ges tillgång till informationen som behöver den för skötsel av sina uppgifter.

7 §. *Tystnadsplikt och förbud mot utnyttjande.* Det är nödvändigt att i lagen ta in en särskild bestämmelse om tystnadsplikt, på grund av de internationella förpliktelseerna om informationssäkerhet gäller också företag samt personer som inte berörs av offentlighetslagen.

Enligt den föreslagna paragrafens 1 mom. är den som är anställd hos en näringsidkare som avses i 1 § 2 mom. skyldig att hemlighålla sådan särskilt känslig information som han eller hon har fått reda på i sitt arbete. Information som omfattas av tystnadsplikten får inte heller röjas efter att anställningsförhållandet har upphört. En person som avses ovan får inte använda sekretessbelagd information till nytta för sig eller någon annan eller till skada för någon annan.

I paragrafens 2 mom. föreslås en hänvisning till offentlighetslagen. Bestämmelsen skall tillämpas på en myndighets anställda och på andra som arbetar hos och utför uppdrag för myndigheten samt på uppdragstagares anställda, så som anges i offentlighetslagens 23 §.

8 §. *Anteckning om säkerhetsklass.* I denna paragraf föreskrivs om säkerhetsklassificering. Enligt paragrafens 1 mom. skall särskilt känsligt informationsmaterial, oberoende av vad som föreskrivs i eller med stöd av lagen om offentlighet i myndigheternas verksamhet, förses med en sådan anteckning om säkerhetsklass som avses i en internationell förpliktelse och som anger vilka krav på informationssäkerhet som skall iaktas vid hanteringen av materialet. Klassificeringen kan anges också på en till handlingen fogad blankett som specificerar denna.

I offentlighetslagens 25 § föreskrivs om situationer där en sekretessanteckning skall göras på en myndighetshandling. I offentlighetsförordningens 2 § föreskrivs om anteckningar som anger säkerhetsklassen. Ingendera bestämmelsen innebär någon skyldighet att anteckna säkerhetsklass. Av denna anledning är det för fullgörande av de internationella förpliktelseerna om informationssäkerhet nödvändigt att i lagen ta in en uttrycklig bestämmelse om saken.

Enligt paragrafens 2 mom. föreskrifter om hur säkerhetsklasserna i en internationell förpliktelse som gäller informationssäkerhet

motsvarar de säkerhetsklasser som iaktas i Finland kan utfärdas genom förordning av statsrådet.

9 §. *Mot säkerhetsklassen svarande hanteringskrav.* En i informationsmaterialet gjord anteckning om säkerhetsklassen anger vilka åtgärder som skall vidtas vid hanteringen av materialet. Säkerhetsåtgärderna förutsätts vara desto strängare ju högre materialets säkerhetsklass är. Paragrafen innebär en allmän förpliktelse att tillämpa de bestämmelser om hantering av informationsmaterial som materialets säkerhetsklass förutsätter.

Enligt paragrafens 1 mom. skall den som producerar, kopierar, överför, distribuerar, förvarar, utplånar eller på annat sätt hanterar särskilt känsligt informationsmaterial se till att materialet skyddas så som dess säkerhetsklass förutsätter.

Paragrafens 2 mom. innehåller ett bemyndigande att genom förordning av statsrådet föreskriva om sådana säkerhetsåtgärder vid hantering av särskilt känsligt informationsmaterial som motsvarar säkerhetsklassificeringen av materialet. Åtgärder som avser informationsskydd omfattar olika tekniska förfaranden som genomförs myndighetsinternt.

10 §. *Säkerhetskrav som gäller utrymmen.* I denna paragraf föreskrivs om en allmän förpliktelse att se till att sådan säkerhetsklassificerad information som avses i lagförslaget förvaras i ändamålsenliga utrymmen. Dessa bestämmelser har ansetts nödvändiga med tanke på de internationella förpliktelseerna. Särskilt känsligt informationsmaterial skall enligt paragrafens 1 mom. förvaras i utrymmen där handlingarna och materialen samt informationen i dem kan skyddas på det sätt som överenskommelsen förutsätter.

Enligt den föreslagna paragrafens 2 mom. kan genom förordning av statsrådet föreskrivas om säkerhetskrav som gäller utrymmen.

11 §. *Utredningar som gäller personsäkerhet samt bedömningar.* Denna paragraf innehåller bestämmelser om personsäkerhet. En sådan personlig säkerhetsutredning som en internationell förpliktelse om informationsäkerhet förutsätter skall enligt 1 mom. göras på det sätt som föreskrivs i och med stöd av lagen om säkerhetsutredningar (177/2002). Sålunda bestäms t.ex. den persons rättigheter som är föremål för utredningen enligt den

nämnda lagen.

I paragrafen föreslås emellertid två bestämmelser som är specialbestämmelser i förhållande till lagen om säkerhetsutredningar. En säkerhetsutredning kan enligt den föreslagna paragrafens *1 mom.* göras också som en begränsad säkerhetsutredning, utan hinder av vad som föreskrivs i 19 § i lagen om säkerhetsutredningar. En förutsättning är att en sådan utredning är nödvändig för att fullgöra en internationell förpliktelse om informationssäkerhet. En begränsad säkerhetsutredning kan sålunda göras också i andra fall än sådana som räknas upp i 19 § i lagen om säkerhetsutredningar. Med beaktande av den nämnda bestämmelsen kan en begränsad säkerhetsutredning göras t.ex. då en person arbetar i utrymmen som tillhör en näringsidkare som har ingått ett säkerhetsklassificerat avtal och då en internationella förpliktelse om informationssäkerhet förutsätter att en sådan utredning görs.

En annan specialbestämmelse i förhållande till lagen om säkerhetsutredningar är *2 mom.* som reglerar myndigheternas befogenheter. Enligt förslaget skall huvudstaben göra en säkerhetsutredning då en sådan behövs för att fullgöra en internationell förpliktelse som gäller försvarsförvaltningen eller anskaffningar av försvarsmateriel. Skyddspolisen skall enligt förslaget se till att andra säkerhetsutredningar som avser personer görs.

Den föreslagna befogenhetsfördelningen motsvarar i huvuddrag den som enligt lagen om säkerhetsutredningar iakttas i fråga om normala eller omfattande säkerhetsutredningar. Den föreslagna bestämmelsen är emellertid exaktare än lagen om säkerhetsutredningar och i den beaktas vilken typ av internationell förpliktelse det är frågan om. Bestämmelsen är också nödvändig på grund av att huvudstaben enligt lagförslagets 12 § föreslås få nya uppgifter, vilket i sin tur försvårar tolkningen av de i lagen om säkerhetsutredningar ingående bestämmelserna om skyddspolisens och huvudstabens befogenheter.

Den föreslagna paragrafens *2 mom.* är också en specialbestämmelse i förhållande till 21 § i lagen om säkerhetsutredningar, som fastställer myndigheternas befogenheter i fråga om begränsade säkerhetsutredningar. Den i

momentet föreslagna befogenhetsfördelningen skall sålunda alltid tillämpas i samband med säkerhetsutredningar som förutsatts av internationella förpliktelser, oberoende av vilken omfattningen av säkerhetsutredningen är.

Enligt 10 § *2 mom.* i lagen om säkerhetsutredningar får den behöriga myndighetens bedömning av tillförlitligheten eller lämpligheten för en tjänst eller ett uppdrag hos den som utredningen gäller inte ingå i en säkerhetsutredning, om inte ett fördrag eller någon annan internationell förpliktelse som avses i lagens 9 § förutsätter det. Eftersom huvudregeln är den att en säkerhetsutredning inte innehåller någon bedömning av en persons tillförlitlighet, nämns i den föreslagna lagen särskilt bedömning av en persons tillförlitlighet. En sådan bedömning skall enligt *3 mom.* på basis av en säkerhetsutredning göras av den nationella säkerhetsmyndigheten eller, om så har överenskommit mellan säkerhetsmyndigheterna, av den för uppgiften utsedda säkerhetsmyndigheten.

Över bedömningen ges ett personligt säkerhetsintyg (Personal Security Clearance). Detta skall normalt tillställas avtalspartens säkerhetsmyndighet på det sätt som anges i överenskommelsen. I lagförslagets 14 § föreskrivs om överlämnande av intyget till vederbörande själv.

12 §. *Säkerhetsutredningar som gäller sammanslutningar samt bedömningar r.* I denna paragraf föreskrivs om utredningar som gäller sammanslutningar. Sådana utredningar görs för att utreda en i lagförslagets 1 § *2 mom.* avsedd näringsidkares tillförlitlighet. Med tillförlitlighet avses här framförallt en bedömning av hur väl näringsidkaren kan skydda säkerhetsklassificerad information. Förfarandet vid säkerhetsutredning och bedömning av en sammanslutning skall sålunda baseras huvudsakligen på information som näringsidkaren själv har lämnat samt på en kartläggning av säkerheten i näringsidkarens verksamhetsutrymmen. Dessa åtgärder skall vidtas enligt ett avtal som ingås med näringsidkaren. Det är sålunda inte, såsom i samband med kontroll av personsäkerhet, fråga om förfaranden som inkräktar på den personliga integriteten.

Enligt *1 mom.* svarar huvudstaben för så-

dana utredningar som avses i paragrafen. Huvudstaben har relativt omfattande erfarenheter av säkerhetsutredningar för företag. Det naturliga alternativet är sålunda att ge huvudstaben uppdraget, innan det närmare har utretts hur det är mest ändamålsenligt att sköta uppgifter som hör till den internationella informationssäkerheten.

I samband med utredningen är det skäl att beakta de omständigheter som anges närmare i momentet. Enligt *1 punkten* skall det utredas hur säkerhetsklassificerad information kan skyddas mot att bli obehörigen röjd, ändrad eller utplånad. Genom utredningen säkerställs informationssäkerheten i olika hanteringskedan. Åtgärderna kan t.ex. innebära att datasystem och informationen i dem skyddas genom att begränsa användarrättigheter.

Enligt *2 punkten* skall det utredas vilka möjligheter det finns att förhindra obehörigt tillträde till utrymmen där säkerhetsklassificerad information hanteras eller där det bedrivs verksamhet som avses i ett säkerhetsklassificerat avtal. Det är sålunda fråga om säkra verksamhetsutrymmen t.ex. genom passagekontroll.

Enligt *3 punkten* skall utredningen utsträckas också till frågan om handledning och utbildning av personalen. Personalen skall bl.a. upplysas om tystnadsplikten och om de förfaranden som skall iakttas vid hanteringen av särskilt känsligt material. En hög informationssäkerhet förutsätter också att det ordnas säkerhetsutbildning för personalen.

Genom utredningen säkerställs å ena sidan att verksamhetsutrymmena och hanteringspraxis är ändamålsenliga, å andra sidan personalens kompetens. Säkerhetsutredningar av en näringsidkares anställda och personer som arbetar i näringsidkarens verksamhetsutrymmen görs på det sätt som föreskrivs i 11 §.

I paragrafens *2 mom.* föreslås en bestämmelse om huvudstabens rätt att på begäran av en näringsidkare göra en säkerhetsutredning och bedömning av en sammanslutning också i andra situationer än sådana som avses i den internationella förpliktelsen om säkerhetsutredning. Huvudstaben kan enligt förslaget göra en säkerhetsutredning och bedömning som gäller en sammanslutning om en näringsidkare har bett om en sådan för

att kunna delta i ett anbudsförfarande som ordnas av en myndighet i en annan stat eller av ett företag som har hemvist i den andra staten. Syftet med bestämmelsen är att trygga finländska företags möjligheter att delta i budsgivningar som förutsätter särskild tillförlitlighet och som genomförs i länder med vilka Finland inte har ingått någon överenskommelse om informationssäkerhet.

Paragrafens *3 mom.* innebär ett bemyndigande att genom förordning av statsrådet utfärda närmare föreskrifter om säkerhetsutredningar som gäller sammanslutningar.

13 §. *Förbindelse om säkerhetsåtgärder.* Enligt den föreslagna paragrafen kan huvudstaben med en näringsidkare som avses i 1 § 2 mom. eller 12 § 2 mom. ingå ett avtal som innebär att näringsidkaren förbinder sig att vidta sådana åtgärder som avses i 12 § 1 mom. samt andra åtgärder för att fullgöra internationella förpliktelser om informationssäkerhet.

I avtalet kan de åtgärder närmare preciseras som näringsidkaren skall genomföra för att uppfylla de krav som följer av internationella förpliktelser om informationssäkerhet. I avtalet förbinder sig näringsidkaren också att göra de eventuella justeringar i sin verksamhet som en säkerhetskartläggning av verksamheten förutsätter. I säkerhetsavtal kan tas in bestämmelser bl.a. om hur långt sekretessplikten sträcker sig, om personalens tystnadsplikt och utbildning, om myndigheternas säkerhetskontroller samt om omständigheter som gäller underleverantörer. I lagens 20 § föreslås en bestämmelse om brott mot förpliktelsen.

Efter en säkerhetsutredning och ett eventuellt avtal kan huvudstaben göra en bedömning av en näringsidkares tillförlitlighet och utfärda ett säkerhetsintyg (Facility Security Clearance).

14 §. *Säkerhetsintyg.* Den säkerhetsmyndighet som på basis av en säkerhetsutredning har gjort en tillförlitlighetsbedömning skall enligt förslaget för den som bedömningen gäller utfärda ett intyg över bedömningen i sådana situationer som avses i den internationella överenskommelsen om informationssäkerhet. Säkerhetsintyg skall, såsom ovan konstateras, i regel tillställas den andra avtalspartens säkerhetsmyndigheter på det sätt

som avses i överenskommelsen. Denna bestämmelse behövs t.ex. för att personen i fråga så som de internationella förpliktelserna förutsätter skall kunna visa att han eller hon har rätt att få tillgång till säkerhetsklassificerad information t.ex. i samband med besök.

Ett intyg skall enligt förslaget utfärdas också för en näringsidkare som har varit föremål för en bedömning på det sätt som avses i 12 § 2 mom. Det är sålunda fråga om en sådan säkerhetsutredning och bedömning av en sammanslutning som inte beror på en internationell förpliktelse om informationssäkerhet utan som har gjorts på näringsidkarens egen begäran.

15 §. *Giltigheten av förpliktelser som gäller informationssäkerhet.* I denna paragraf föreskrivs hur långt de i kapitlet reglerade förpliktelserna sträcker sig tidsmässigt. Enligt förslaget skall kapitlets bestämmelser tillämpas också då den överenskommelse eller författning som tillämpningen av bestämmelserna baserar sig på inte längre är i kraft. Tillämpningen fortsätter så länge som det är nödvändigt med tanke på det allmänna intresse som ligger till grund för säkerhetsklassificeringen.

I fråga om sekretesspliktens upphörande gäller vad som föreskrivs i lagen om offentlighet i myndigheternas verksamhet. Enligt offentlighetslagens 31 § är huvudregeln den att sekretessen för en handling upphör då 25 år har förflutit från det att handlingen upprättades. Statsrådet kan under vissa förutsättningar förlänga sekretesstiden. Försvarsministeriet har gjort en framställning till justitje ministeriet om en sådan ändring av bestämmelserna om sekretesstiden att denna skall bestämmas med beaktande av behovet att skydda sekretessbelagd information om byggnader och anordningar under en så lång tid som byggnaderna och anordningarna är i användning. Avsikten är att i detta sammanhang också utreda om det är nödvändigt att precisera dessa bestämmelser med beaktande av de internationella förpliktelserna om informationssäkerhet.

4 kap. Särskilda bestämmelser

16 §. *Informationsskyldighet.* I paragrafens 1 mom. föreskrivs om den informationsskyld-

dighet som gäller för myndigheter och i paragrafens 2 mom. om den informationsskyldighet som gäller för näringsidkare. Syftet med bestämmelserna är att säkerställa att behöriga säkerhetsmyndigheter får den information som de behöver för att sköta sina nya uppgifter.

En myndighet skall enligt föreslagna 1 mom., utan hinder av sekretessbestämmelserna, på begäran ge utrikesministeriet, försvarsministeriet, huvudstaben och skyddspolisen den information som de behöver för att göra en säkerhetsutredning som avses i en internationell överenskommelse om informationssäkerhet och för en bedömning som baseras på en sådan utredning.

Enligt den föreslagna lagen skall näringsidkare göras föremål för en säkerhetsutredning om de kan få tillgång till säkerhetsklassificerad information t.ex. då de deltar i en anbudsgivning som gäller en annan stats försvarsmateriel. För att den myndighet som svarar för utredningen skall kunna fullgöra sin uppgift skall näringsidkaren enligt föreslagna 2 mom. ge den information som behövs för ändamålet. En näringsidkare måste också ge tillträde till sina utrymmen då detta är nödvändigt för utredningen eller för att uppfylla den inspektions- och övervakningsskyldighet som följer av en internationell förpliktelse om informationssäkerhet.

17 §. *Rätt att lämna ut sekretessbelagd information.* I denna paragraf föreskrivs om utlämnande av sekretessbelagd information till en annan avtalspart, för samarbete som är baserat på en internationell förpliktelse om informationssäkerhet.

Enligt förslaget har finska myndigheter rätt att lämna ut handlingar och uppgifter som är nödvändiga för verksamhet som avses i avtalet eller för genomförande av ett program som baserar sig på avtalet, utan hinder av vad som i Finlands lagstiftning föreskrivs om sekretessbeläggning av handlingar och information. Detta gäller inte information som skall sekretessbeläggas på grund av integritetsskydd. Det är sålunda inte möjligt att t.ex. under en annan avtalsparts besök ge tillträde till register som används för personliga säkerhetsutredningar.

18 §. *Besök av representanter för internationella organ och fördragslutande stater.*

Enligt paragrafens 1 mom. har en myndighet rätt att inom ramen för en internationell förpliktelse om informationssäkerhet låta representanter för internationella organisationer och organ samt för fördragsslutande stater bekanta sig med sina säkerhetsarrangemang och verksamhetsutrymmen oberoende av vad som föreskrivs om sekretessbeläggning av säkerhetsarrangemang eller vad som föreskrivs eller bestäms om tillträde till utrymmen där sekretessbelagd information hantteras eller förvaras.

I paragrafens 2 mom. föreskrivs om en i lagförslaget 1 § 2 mom. avsedd näringsidkares skyldighet att tillåta att representanter för myndigheter och internationella organ eller fördragsslutande stater bekanta sig med näringsidkarens säkerhetsarrangemang och verksamhetsutrymmen då detta är nödvändigt för att uppfylla en internationell förpliktelse som gäller informationssäkerhet.

Besök inom ramen för internationella förpliktelser om informationssäkerhet är inte jämförbara med inspektionsrätt som har beviljats en främmande stats myndighet, utan de utgör en del av det normala internationella samarbetet i ärenden som gäller informationssäkerhet. Ett besök förutsätter närvaro och medverkan av den finska säkerhetsmyndigheten. Därför anses i denna proposition att bedömningen inte innefattar självständig beslutanderätt som är bindande för Finland. Det är sålunda enligt propositionen inte fråga om sådana övervakningsåtgärder av en utländsk myndighet på finskt territorium som innebär offentlig maktutövning i strid med grundlagen (GrUU 179/1997).

19 §. *Utredning av och anmälan om förseelser.* Den nationella säkerhetsmyndigheten skall enligt förslaget i sådana fall som avses i en internationell förpliktelse om informationssäkerhet underrätta den andra avtalsparten om det har kommit till dess kännedom att skyddet av säkerhetsklassificerad information har äventyrats och bestämmelser om informationssäkerhet har överträtts samt vidta åtgärder för att utreda ärendet och väcka åtal mot de skyldiga. Bestämmelsen behövs på grund av artikel 6 i ESA-överenskommelsen om informationssäkerhet och artikel 10 i överenskommelsen mellan Finland och Tyskland.

20 §. *Straffbestämmelser.* I denna paragraf föreslås bestämmelser om straffbarhet för gärningar som strider mot bestämmelserna om handlingssekretess och tystnadsplikt. Enligt paragrafens 1 mom. skall den som bryter mot vad som i den föreslagna lagens 6 § föreskrivs som handlingssekretess eller i 7 § om tystnadsplikt och nyttjandeförbud dömas till straff enligt strafflagens 40 kap 5 §, om gärningen inte är straffbar enligt strafflagens 38 kap. 1 eller 2 § eller om strängare straff inte föreskrivs i någon annan lag. Om en tjänsteman på något annat sätt bryter mot de i lagen angivna förpliktelseerna skall gärningen bedömas enligt vad som i strafflagen föreskrivs om tjänstebrott. Det kan då bli fråga om att tillämpa vad som i strafflagens 40 kap. föreskrivs t.ex. om missbruk av tjänsteställning eller brott mot tjänsteplikt.

Enligt paragrafens 2 mom. skall också brott mot en sådan förbindelse som avses i 13 § anses som brott mot tystnadsplikten. Bestämmelsen skall enligt förslaget tillämpas på en näringsidkare som bryter mot ett med en myndighet ingånget avtal om vidtagande av åtgärder som gäller informationssäkerhet.

5 kap. **Ikraftträdelsebestämmelser**

21 §. *Ikraftträdande.* Avsikten är att den föreslagna lagen skall träda i kraft så snart som möjligt efter att den har godkänts och stadsfästs. Åtgärder som verkställandet av lagen förutsätter kan vidtas också innan lagen träder i kraft.

3. **Närmare bestämmelser**

Den föreslagna lagen om internationella förpliktelser som gäller informationssäkerhet innehåller ett bemyndigande att utfärda bestämmelser genom förordning av statsrådet (lagförslag nr 3, 4 § 2 mom., 8 § 2 mom., 9 § 2 mom., 10 § 2 mom., och 12 § 2 mom.). Dessa bestämmelser gäller huvudsakligen säkerhetsarrangemang av teknisk karaktär.

4. **Ikraftträdande**

Överenskommelsen mellan Finland och Tyskland träder i kraft femton dagar efter att Finland har meddelat Tyskland att de natio-

nella åtgärder som behövs för överenskommelsens ikraftträdande har vidtagits. Med tanke på den finländska industrins möjligheter till deltagande är det viktigt att detta sker under våren 2004.

ESA-överenskommelsen om informationssäkerhet trädde i kraft internationellt den 20 juni 2003. Överenskommelsen träder för Finlands del i kraft trettio dagar efter det att Finland har deponerat sina ratifikationsinstrument.

Avsikten är att lagarna om ikraftsättande av överenskommelserna skall träda i kraft vid en tidpunkt som bestäms genom förordning av republikens president, samtidigt som överenskommelserna träder i kraft för Finlands del.

Avsikten är att lagen om internationella förpliktelser som gäller informationssäkerhet skall träda i kraft så snart som möjligt efter att den har antagits och stadsfästs.

5. Riksdagens samtycke samt behandlings- och lagstiftningsordningen

5.1. Riksdagens samtycke

Enligt grundlagens 94 § 1 mom. krävs riksdagens godkännande för fördrag och andra internationella förpliktelser som innehåller sådana bestämmelser som hör till området för lagstiftningen. Enligt grundlagsutskottets tolkningspraxis anses en bestämmelse 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 något annat avseende gäller grunderna för individens rättigheter och skyldigheter, om den sak som bestämmelsen gäller enligt grundlagen skall föreskrivas i lag eller om det finns lagbestämmelser om den sak som lagen gäller eller om det enligt rådande uppfattning i Finland skall lagstiftas om saken. Grundlagsutskottet anser att enligt dessa kriterier hör en bestämmelse om en internationell förpliktelse till området för lagstiftningen oavsett om den strider mot eller överensstämmer med en lagbestämmelse i Finland (se t.ex. GrUU 11/2000 rd och GrUU 12/2000 rd).

På de grunder som nämns ovan är flera be-

stämmelser i de internationella överenskommelser som ingår i propositionen sådana att de kräver riksdagens godkännande. *Artikel 1 i överenskommelsen om skydd för och utbyte av Europeiska rymdorganets säkerhetsklassificerade information* innehåller en definition av begreppet klassificerad information. En avtalsbestämmelse som indirekt påverkar tolkningen och tillämpningen av sådana materiella avtalsbestämmelser som hör till området för lagstiftningen hör också de till området för lagstiftningen (GrUU 6/2001 rd).

Enligt överenskommelsens *artikel 2* skall de fördragsslutande parterna, i enlighet med överenskomna säkerhetsprinciper och minimistandarder för dokumentssäkerhet, skydda säkerhetsklassificerad information som härstammar från ESA eller som överlämnats till ESA av en medlemsstat och som är märkt som sådan. I Finland är huvudregeln den att myndighetshandlingar är offentliga. Enligt grundlagens 12 § 2 mom. har var och en rätt att ta del av offentliga myndighetshandlingar. Denna rätt kan begränsas endast genom lag.

Överenskommelsens *artikel 4* innehåller bestämmelser om de fördragsslutande parternas skyldighet att säkerhetskontrollera personer som har eller kan få tillgång till sådan säkerhetsklassificerad information som avses i överenskommelsen. Personliga säkerhetsutredningar skall göras med beaktande av vad som i grundlagens 10 § 1 mom. föreskrivs om skydd för privatlivet och skyldigheten att utfärda närmare bestämmelser om skydd för personuppgifter genom lag. I lagen om säkerhetsutredningar (177/2002) föreskrivs om personliga säkerhetsutredningar i Finland samt om utredningsförfarandet.

Enligt överenskommelsens *artikel 6* skall de fördragsslutande parterna undersöka alla fall där det konstateras eller misstänks att sådan information som avses i avtalet har äventyrats eller förlorats. Finska myndigheter har inte någon allmän skyldighet att undersöka fall där säkerhetsklassificerad information har äventyrats eller förlorats. Det är fråga om att påföra myndigheterna en ny skyldighet. För att bestämmelsen skall kunna verkställas måste det föreskrivas om denna skyldighet genom lag. En bestämmelse om saken föreslås i lagen om internationella förpliktelser som gäller informationssäkerhet

(lagförslag nr 3, 19 §).

Överenskommelsens *artikel 7* uppställer för medlemsstaten och rådet samt för ESA:s generaldirektör en skyldighet att i enlighet med ESA-konventionen avstå från immuniteten i sådana fall där en representant för en medlemsstat, ESA:s generaldirektör eller en medlem av personalen eller någon av ESA:s experter är part i en rättsprocess som gäller obehörigt röjande av säkerhetsklassificerad information. Enligt grundlagens 80 § skall genom lag utfärdas bestämmelser om grunderna för individens rättigheter och skyldigheter. Grundlagsutskottet har betonat att avtalsbestämmelser som gäller privilegier och immunitet hör till området för lagstiftningen (GrUU 38/2000 rd, GrUU 49/2001). Också en avtalsbestämmelse som i vissa situationer förutsätter avstående från privilegier eller immunitet kan anses förutsätta riksdagens godkännande.

I *artiklarna 2 och 6 i överenskommelsen mellan Finland och Tyskland om ömsesidigt skydd för säkerhetsklassificerad information* definieras begreppen klassificerad information och klassificerade avtal. Eftersom dessa bestämmelser i överenskommelsen indirekt kan påverka tolkningen och tillämpningen av sådana materiella bestämmelser i överenskommelsen som hör till området för lagstiftningen, förutsätter de riksdagens godkännande (GrUU 6/2001 rd).

Enligt *artiklarna 4.1. och 4.2* skall den behöriga myndigheten i den mottagande staten eller den som verkar på uppdrag av denna förse den klassificerade information som har förmedlats med en säkerhetsklassificering som motsvarar den nationella klassificeringen. I offentlighetslagen föreskrivs hur anteckningar om sekretess och klassificering görs i Finland. Enligt lagens 25 § skall anteckning om sekretess göras i en sekretessbelagd myndighetshandling som ges ut till en part och som skall vara sekretessbelagd på grund av någon annans eller allmänt intresse. Anteckning kan enligt prövning göras även på andra sekretessbelagda handlingar. Bestämmelserna i överenskommelsen ställer sålunda strängare krav än Finlands lagstiftning på säkerhetsklassificering av information. Överenskommelsens bestämmelser påverkar direkt också tillämpningen av sådana materi-

ella bestämmelser i överenskommelsen som hör till området för lagstiftningen, såsom vilket informationsmaterial som omfattas av överenskommelsen och de förpliktelser som följer av denna. Bestämmelserna förutsätter sålunda riksdagens godkännande.

Enligt *artikel 5* skall de fördragsslutande parterna inom ramen för sin egen lagstiftning vidta alla nödvändiga åtgärder för att skydda sådan klassificerad information som har förmedlats på basis av denna överenskommelse eller som har producerats i anslutning till ett klassificerat avtal. Dessa åtgärder inkluderar begränsningar som gäller förmedling och användning av samt tillgång till sådan information. Enligt grundlagens 12 § 2 mom. är handlingar som innehas av myndigheterna offentliga om inte offentligheten av tvingande skäl särskilt har begränsats genom lag.

I *artikel 8* föreskrivs att de båda fördragsslutande parterna skall tillåta att den andra fördragsslutande partens representanter eller uppdragstagares personal gör sådana besök hos den egna statens ämbetsverk och inrättningar och uppdragstagares ("contractors") verksamhetsutrymmen som innebär att besökarna får tillgång till klassificerad information.

Syftet med besök som görs av en fördragsslutande parts representanter är att säkerställa att säkerhetsklassificerad information skyddas på det sätt som avses i överenskommelsen. Denna besöksrätt innebär inte sådan offentlig maktutövning eller inspektionsrätt som skulle strida mot grundlagen (GrUU 179/1997).

Bestämmelsen innebär indirekt också för enskilda uppdragstagare en skyldighet att tillåta besök i sina egna verksamhetsutrymmen. I detta avseende är det skäl att betrakta grundlagens 80 § enligt vilken genom lag skall utfärdas bestämmelser om grunderna för individens rättigheter och skyldigheter. Med stöd av denna grundlagsbestämmelse är det motiverat att genom lag utfärda bestämmelser om förpliktelser som gäller också enskilda juridiska personer.

Artikel 10 förutsätter att den andra fördragsslutande parten omedelbart skall underlättas i det fall att möjligheten till obehörigt röjande av säkerhetsklassificerad information inte kan uteslutas eller om obehörigt röjande

misstänks eller har konstaterats (10.1). Den fördragsslutande partens behöriga myndigheter och domstolar skall dessutom i enlighet med sin nationella lagstiftning undersöka brott mot bestämmelserna om skyddet av säkerhetsklassificerad information samt vidta rättsliga åtgärder.

I Finlands lagstiftning finns för närvarande inga bestämmelser om sådana skyldigheter som avses i artikeln. Med tanke på bestämmelsens verkställighet är det skäl att genom lag utfärda bestämmelser om myndigheternas skyldigheter i detta avseende. I den föreslagna lagen om internationella förpliktelser som gäller informationssäkerhet föreslås en bestämmelse om saken (lagförslag nr 3, 19 §).

5.2. Behandlings- och lagstiftningsordning

Bestämmelser som är relevanta för behandlingsordningen är artikel 2 i överenskommelsen om skydd för och utbyte av Europeiska rymdorganets säkerhetsklassificerade information samt artikel 5 i överenskommelsen mellan Finland och Tyskland om ömsesidigt skydd för säkerhetsklassificerad information. Dessa bestämmelser ställer exaktare sekretesskrav än Finlands gällande lagstiftning, men de kan inte anses utvidga området för sekretessen.

Överenskommelsernas sekretessbestämmelser kan anses förutsätta nationell lagstiftning så som avses i grundlagens 12 § 2 mom. Det finns ett vägande samhälleligt intresse av sådana sekretessbestämmelser för att trygga Finlands och finländska företags möjligheter att delta i sådana internationella och bilaterala verksamheter och projekt som kan förutsätta utbyte av känslig information. Det kan också konstateras att grundlagsutskottet i sitt utlåtande med anledning av regeringens proposition om godkännande av vissa bestämmelser i säkerhetsskyddsavtalet mellan Finland och Västeuropeiska unionen (GrUU 39/1997 rd) ansåg att det med tanke på syftet med avtalet, dvs. att göra det möjligt för Finland att samarbeta med VEU, kan anses nöd-

vändigt att begränsa offentlighetsprincipen på det sätt som avses i avtalet. Sekretessintresset stämmer också överens med de grunder som nämns i offentlighetslagen. Enligt regeringens uppfattning berör överenskommelsen inte på ett sådant sätt den allmänna rätten till information att den kränker offentlighetsprincipen som framgår av grundlagens 12 § 2 mom.

På de grunder som nämns ovan kan det anses att överenskommelsen om skydd för och utbyte av Europeiska rymdorganets säkerhetsklassificerade information och överenskommelsen mellan Finland och Tyskland om ömsesidigt skydd för säkerhetsklassificerad information inte innehåller bestämmelser som berör grundlagen på det sätt som avses i grundlagens 94 § 2 mom. och 95 § 2 mom. Enligt regeringens åsikt kan överenskommelserna sålunda godkännas med enkel majoritet och förslagen till sättande i kraft av de bestämmelser i överenskommelserna som hör till området för lagstiftningen samt till lag om internationella förpliktelser som gäller informationssäkerhet kan godkännas i vanlig lagstiftningsordning.

Med stöd av det som anförs ovan och i enlighet med grundlagens 94 § föreslås

1) att Riksdagen godkänner överenskommelse som den 19 augusti 2002 ingicks i Paris mellan parterna i konventionen om uppriktandet Europeiska rymdorganet och Europeiska rymdorganet om skydd för och utbyte av säkerhetsklassificerad information, samt

2) att Riksdagen godkänner den överenskommelse som den 25 februari 2004 ingicks i Helsingfors mellan Republiken Finland och Tyska förbundsrepubliken om ömsesidigt skydd för säkerhetsklassificerad information.

Eftersom de nämnda överenskommelserna innehåller bestämmelser som hör till området för lagstiftningen överlämnas till riksdagen samtidigt följande lagförslag:

*Lagförslag***1.****Lag**

om sättande i kraft av de bestämmelser som hör till området för lagstiftningen i överenskommelsen mellan parterna i konventionen om upprättandet av Europeiska rymdorganet och Europeiska rymdorganet om skydd för och utbyte av säkerhetsklassificerad information

I enlighet med riksdagens beslut föreskrivs:

1 §
De bestämmelser som hör till området för lagstiftningen i den överenskommelse som ingicks i Paris den 19 augusti 2002 mellan parterna i konventionen om upprättandet av Europeiska rymdorganet samt Europeiska rymdorganet om skydd för och utbyte av sä-

herhetsklassificerad information gäller som lag, sådana Finland har förbundit sig till dem.

2 §
Om ikraftträdandet av denna lag bestäms genom förordning av republikens president.

2.**Lag**

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

I enlighet med riksdagens beslut föreskrivs:

1 §
De bestämmelser som hör till området för lagstiftningen i den överenskommelse som ingicks i Helsingfors den 25 februari 2004 mellan republiken Finland och Tyska förbundsrepubliken om ömsesidigt skydd för säkerhetsklassificerad information gäll-

er som lag, sådana Finland har förbundit sig till dem.

2 §
Om ikraftträdandet av denna lag bestäms genom förordning av republikens president.

3.

Lag**om internationella förpliktelser som gäller informationssäkerhet**

I enlighet med riksdagens beslut föreskrivs:

1 kap.

Allmänna bestämmelser

1 §

Lagens tillämpningsområde

I denna lag föreskrivs om myndigheternas åtgärder för att uppfylla internationella förpliktelser som gäller informationssäkerhet.

Lagen tillämpas också på en näringsidkare och dennas anställda i sådana fall då näringsidkaren är part i ett säkerhetsklassificerat avtal eller deltar i ett upphandlingsförfarande innan ett sådant avtal sluts eller är underleverantör för en sådan näringsidkare.

Lagens 12–14 § samt 16 § 2 mom. tillämpas också på en näringsidkare som begär en utredning över sin tillförlitlighet och en bedömning på basis av utredningen för att kunna delta i ett anbudsförfarande som ordnas av en myndighet i en annan stat eller av ett företag som har hemvist i den andra staten.

2 §

Definitioner

I denna lag avses med

1) *internationell förpliktelse som gäller informationssäkerhet* sådana bestämmelser i internationella överenskommelser som är bindande för Finland som gäller åtgärder för skydd av särskilt känsligt material samt andra

förpliktelser för Finland som skall iakttas av Finland och gäller nämnda åtgärder,

2) *särskilt känsligt informationsmaterial* 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,

3) *säkerhetsklassificerat avtal* 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.

3 §

Förhållande till annan lagstiftning

I fråga om offentlighet för särskilt känsligt informationsmaterial och god informationshantering av materialet gäller lagen om offentlighet i myndigheternas verksamhet (621/1999) och vad som bestäms med stöd av den, om inte något annat föreskrivs i denna lag.

En på lagen om offentlighet i myndigheternas verksamhet eller på någon annan lag ba-

serad begäran om att få uppgifter ur särskilt känsligt informationsmaterial skall handläggas och avgöras av den myndighet till vilken informationsmaterialet har sänts eller som skall behandla ärendet i dess helhet.

2 kap.

Säkerhetsmyndigheterna och samarbetet mellan dem

4 §

Den nationella säkerhetsmyndigheten och de utsedda säkerhetsmyndigheterna

Utrikesministeriet är Finlands nationella säkerhetsmyndighet vid uppfyllandet av internationella förpliktelser som gäller informationssäkerhet. Försvarsministeriet, huvudstaben och skyddspolisen kan verka som sådana utsedda säkerhetsmyndigheter som avses i internationella förpliktelser som gäller informationssäkerhet. Skyddspolisen och huvudstaben ser till att säkerhetsutredningar görs i enlighet med 11 och 12 §.

Föreskrifter om uppgiftsfördelningen mellan säkerhetsmyndigheterna kan utfärdas genom förordning av statsrådet.

5 §

Informationsutbyte och samarbete mellan säkerhetsmyndigheterna

De säkerhetsmyndigheter som avses i 4 § skall samarbeta för att på ett ändamålsenligt sätt uppfylla internationella förpliktelser som gäller informationssäkerhet samt i detta syfte utbyta information, utan hinder av bestämmelserna om sekretess.

Utän hinder av vad som föreskrivs i 4 § 1 mom. samt i 11–13 § kan den nationella säkerhetsmyndigheten och de utsedda säkerhetsmyndigheterna avtala om att sköta en viss uppgift eller ett visst uppgiftsområde för den andra säkerhetsmyndighetens räkning, om ett sådant arrangemang behövs för att

uppgifterna skall kunna skötas på ett ändamålsenligt, ekonomiskt och flexibelt sätt.

3 kap.

Åtgärder som gäller informationssäkerhet

6 §

Sekretess och användning av information

Särskilt känsligt informationsmaterial skall sekretessbeläggas.

Särskilt känsligt informationsmaterial får användas och lämnas ut endast för angivet ändamål, om inte den som bestämt materialets säkerhetsklass har samtyckt till något annat.

En myndighet som hanterar särskilt känsligt informationsmaterial skall se till att endast personer som behöver informationen för skötsel av sina uppgifter har tillgång till materialet. Dessa personer skall i de fall som den internationella förpliktelsen som gäller informationssäkerhet förutsätter namnges på förhand. Detsamma gäller näringsidkare som avses 1 § 2 mom.

7 §

Tystnadsplikt och förbud mot utnyttjande

Den som är anställd hos en näringsidkare som avses 1 § 2 mom. är skyldig att hemlighålla vad han eller hon i detta uppdrag fått veta om uppgifter som ingår i särskilt känsligt informationsmaterial. Information som omfattas av tystnadsplikten får inte heller röjas efter att anställningen upphört. En person som avses ovan får inte använda sekretessbelagd information för att skaffa sig själv eller någon annan fördel eller för att skada någon annan.

I fråga om tystnadsplikten för den som är anställd hos eller annars verkar hos en myndighet, den som verkar på uppdrag av en myndighet eller är anställd hos den som utgör uppdraget samt i fråga om förbud mot utnyttjande samband därmed gäller vad som föreskrivs i lagen om offentlighet i myndigheternas verksamhet.

8 §

Anteckning om säkerhetsklass

Särskilt känsligt informationsmaterial skall oberoende av vad som föreskrivs i lagen om offentlighet i myndigheternas verksamhet eller med stöd av den försees med en sådan anteckning om säkerhetsklass som anges i en internationell förpliktelse som gäller informationssäkerhet och som anger vilka säkerhetskrav som skall iaktas vid hanteringen av materialet. Anteckningen kan göras också på en till handlingen fogad blankett som specificerar handlingen.

Föreskrifter om hur säkerhetsklasserna i en internationell förpliktelse som gäller informationssäkerhet motsvarar de säkerhetsklasser som iaktas i Finland kan utfärdas genom förordning av statsrådet.

9 §

Mot säkerhetsklassen svarande hanteringskrav

När särskilt känsligt informationsmaterial produceras, kopieras, översänds, distribueras, lagras, utplånas eller hanteras i något annat avseende, skall skyddas på ett sätt som motsvarar säkerhetsklassen.

Föreskrifter om sådana mot olika säkerhetsklasser svarande säkerhetsåtgärder som skall vidtas vid hantering av särskilt känsligt informationsmaterial kan utfärdas genom förordning av statsrådet.

10 §

Säkerhetskrav som gäller utrymmen

Särskilt känsligt informationsmaterial skall 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.

Föreskrifter om säkerhetskrav för sådana utrymmen som avses i 1 mom. kan utfärdas genom förordning av statsrådet.

11 §

Utredningar som gäller personsäkerhet samt bedömningar

En säkerhetsutredning som läggs till grund för bedömning av en persons tillförlitlighet, enligt vad som förutsätts i en internationell förpliktelse som gäller informationssäkerhet, skall göras på det sätt som föreskrivs i lagen om säkerhetsutredningar (177/2002) och med stöd av den. Utan hinder av 19 § i nämnda lag är det också möjligt att göra en säkerhetsutredning som en begränsad säkerhetsutredning, om en sådan behövs för att uppfylla den internationella förpliktelsen om informationssäkerhet.

Säkerhetsutredningen skall göras av huvudstaben då en sådan utredning behövs för att uppfylla en internationell förpliktelse som gäller försvarsförvaltningen eller anskaffningar av försvarsmateriel. Skyddspolisen ser till att andra säkerhetsutredningar som avser personer görs.

På basis av säkerhetsutredningen bedöms en persons tillförlitlighet av den nationella säkerhetsmyndigheten eller, om så har avtalats mellan säkerhetsmyndigheterna, av den för uppgiften utsedda säkerhetsmyndigheten.

12 §

Säkerhetsutredningar som gäller sammanslutningar samt bedömningar

Huvudstaben svarar med stöd av en internationell förpliktelse som gäller informationssäkerhet för utredningen av en sådan näringsidkares tillförlitlighet som avses i 1 § 2 mom. (*säkerhetsutredning som gäller sammanslutning*) samt för bedömningen på basis av utredningen, om något annat inte har avtalats mellan säkerhetsmyndigheterna. Vid utredningen och bedömningen skall det beaktas hur

1) säkerhetsklassificerad information skyddas mot att bli obehörigen röjd, ändrad eller utplånad,

2) obehörigt tillträde kan förhindras till utrymmen där säkerhetsklassificerad informa-

tion hanteras eller verksamhet bedrivs enligt ett säkerhetsklassificerat avtal,

3) handledningen och utbildningen av personalen är ordnad.

Huvudstaben kan göra en säkerhetsutredning som gäller en sammanslutning samt en bedömning då en näringsidkare har bett om en sådan för att kunna delta i ett anbudsförvarande som ordnas av en myndighet i en annan stat eller av ett företag som har hemvist i den andra staten.

Närmare föreskrifter om en säkerhetsutredning som gäller sammanslutning kan utfärdas genom förordning av statsrådet.

13 §

Förbindelse om att vidta säkerhetsåtgärder

Huvudstaben kan med en näringsidkare som avses i 1 § 2 mom. eller i 12 § 2 mom. ingå ett avtal om att näringsidkaren förbinder sig att vidta sådana åtgärder som avses i 12 § 1 mom. samt andra åtgärder som är nödvändiga för att uppfylla internationella förpliktelser om informationssäkerhet.

14 §

Säkerhetsintyg

En säkerhetsmyndighet som på basis av en säkerhetsutredning har gjort en bedömning av en persons tillförlitlighet skall ge den som bedömningen avser ett intyg över bedömningen, om en internationell förpliktelse som gäller informationssäkerhet förutsätter detta. Ett sådant intyg skall ges också en näringsidkare som har varit föremål för en sådan bedömning som avses i 12 § 2 mom.

15 §

Giltigheten av förpliktelser som gäller informationssäkerhet

Bestämmelserna i detta kapitel skall tillämpas så länge det är nödvändigt på grund av det allmänna intresse som säkerhetsklassificeringen baserar sig på, också då den överenskommelse eller den författning som tillämpningen av bestämmelserna baserar sig

på inte längre är i kraft. I fråga om när sekretessen upphör gäller vad som föreskrivs i lagen om offentlighet i myndigheternas verksamhet.

4 kap.

Särskilda bestämmelser

16 §

Informationsskyldighet

Utän hinder av sekretessbestämmelserna skall en myndighet på begäran ge huvudstaben och skyddspolisen information som behövs för sådan säkerhetsutredning som avses i en internationell överenskommelse om informationssäkerhet och för en bedömning som baseras på en sådan utredning.

En näringsidkare som avses i 1 § 2 och 3 mom. skall ge den behöriga säkerhetsmyndigheten den information som behövs för en säkerhetsutredning eller inspektion eller som annars behövs för att uppfylla internationella förpliktelser om informationssäkerhet, samt i detta syfte ge utredare och inspektörer tillträde till sina verksamhetsutrymmen.

17 §

Rätt att lämna ut sekretessbelagd information

Finska myndigheter har rätt att till en annan fördragsslutande part lämna ut handlingar och information som behövs för uppfyllande av en internationell förpliktelse som gäller informationssäkerhet, utan hinder av vad som i finsk lagstiftning föreskrivs om sekretessbeläggning av handlingar och uppgifter. Vad som föreskrivs ovan gäller inte uppgifter som är sekretessbelagda för tryckande av integritetsskydd.

18 §

Besök av representanter för internationella organ och för fördragsslutande stater

En myndighet har rätt att inom ramen för en internationell förpliktelse som gäller

informationssäkerhet låta representanter för internationella organisationer och organ samt för fördragsslutande stater bekanta sig med sina säkerhetsarrangemang och verksamhetsutrymmen oberoende av vad som föreskrivs om sekretessbeläggning av säkerhetsarrangemangen eller vad som föreskrivs om tillträde till utrymmen där sekretessbelagd information hanteras eller förvaras.

En näringsidkare som avses i 1 § 2 mom. skall tillåta att representanter för myndigheter, internationella organ och fördragsslutande stater bekantar sig med näringsidkarens säkerhetsarrangemang och verksamhetsutrymmen, när det är nödvändig för att uppfylla en internationell förpliktelse som gäller informationssäkerhet.

19 §

Utredning av och anmälan om förseelser

Den nationella säkerhetsmyndigheten skall i sådana fall som avses i en internationell förpliktelse som gäller informationssäkerhet underrätta den andra fördragsslutande parten om sådant äventyrande av skyddet för säkerhetsklassificerad information och om sådant överträdande av bestämmelse om informationssäkerhet som myndigheten fått kännedom om, samt vidta åtgärder för att utreda

ärendet och väcka åtal mot den som gjort sig skyldig till en straffbar gärning.

20 §

Straffbestämmelser

Straff för brott mot skyldigheten att sekretessbelägga handlingar enligt 6 § och för brott mot tystnadsplikten och förbudet mot utnyttjandet enligt 7 § döms ut enligt 40 kap. 5 § strafflagen (39/1889), om inte gärningen utgör brott enligt 38 kap. 1 eller 2 § strafflagen eller om inte strängare straff för gärningen föreskrivs någon annanstans i lag.

Som brott mot tystnadsplikten enligt 1 mom. anses också brott mot en förbindelse som avses i 13 §.

5 kap.

Ikraftträdelsebestämmelser

21 §

Ikraftträdande

Denna lag träder i kraft den 200 .
Åtgärder som verkställigheten av lagen förutsätter får vidas innan lagen träder i kraft.

Helsingfors den 30 april 2004

Republikens President

TARJA HALONEN

Minister *Leena Luhtanen*

*Bilagor***Bilaga 1: Överenskommelse mellan parterna i konventionen om upprättandet av Europeiska rymdorganet samt Europeiska rymdorganet om skydd för och utbyte av säkerhetsklassificerad information (översättning till svenska)**

De stater som är parter i konventionen om upprättandet av Europeiska rymdorganet (ESA) samt Europeiska rymdorganet, nedan "de fördragsslutande parterna", som

- BEAKTAR konventionen om upprättandet av Europeiska rymdorganet (nedan kallad ESA-konventionen), som trädde i kraft den 30 oktober 1980, och särskilt artiklarna III och XI.5. m i konventionen,

- BEAKTAR kapitel VI reglerna om information och immateriell äganderätt, ESA/C/CLV/Regler 5 (Final), som godkänkts av rådet den 19 december 2001,

- ERKÄNNER att åtgärder för främjande av samarbetet mellan medlemsstaterna på området rymdforskning och -teknologi och rymdtillämpningar kan kräva utbyte av säkerhetsklassificerad information och tillhörande material mellan de fördragsslutande parterna,

- OBSERVERAR nödvändigheten att uppnå en tillfredsställande skyddsnivå för den av säkerhetsklassificerade informationen inom organet och dess medlemsstater och behovet att därför inrätta ett lämpligt rättsligt instrument, så som konstateras i ESA-rådets resolution om inrättande av en arbetsgrupp för informationssäkerhet som har godkänkts av rådet med stöd av ESA/C/CLI/Res. 8 (final),

har kommit överens om följande:

Artikel 1

Med säkerhetsklassificerad information avses i denna överenskommelse uppgifter, handlingar eller material, oberoende av formen, vars obehöriga röjande kan skada en eller flera fördragsslutande parter intressen

och som försetts med en säkerhetsklassificering.

Artikel 2

De fördragsslutande parterna:

1. Skyddar och bevarar, i enlighet med överenskomna säkerhetsprinciper och minimistandarder för dokumentssäkerhet,

a) klassificerad information som härstammar från ESA eller som överlämnas till ESA av en medlemsstat och som är märkt som sådan,

b) klassificerad information som härstammar från en medlemsstat och som överlämnas till en annan medlemsstat till stöd för ett ESA-program, -projekt eller -avtal och som är märkt som sådan.

2. Upprätthåller den säkerhetsklassificering av information som anges i 1 punkten och skyddar informationen i enlighet därmed;

3. Använder den säkerhetsklassificerade informationen på det sätt som anges i 1 punkten endast för de ändamål som anges i ESA-konventionen och de beslut och resolutioner som hänförs till konventionen;

4. Avslöjar inte sådan information som avses i 1 punkten till stater som inte är parter i ESA-konventionen eller organ som lyder under deras jurisdiktion eller till någon annan internationell organisation utan ett skriftligt förhandsgodkännande av den som tillhandahåller informationen.

Artikel 3

De fördragsslutande parterna genomför ESA:s normer för dokumentssäkerhet för att säkerställa en enhetlig skyddsnivå för den säkerhetsklassificerade informationen.

Artikel 4

1. De stater som är fördragsslutande parter säkerställer att över de medborgare, som under skötsel av sina tjänsteuppgifter, eller de vars tjänsteplikter eller funktioner kan medge tillgång, behöver få tillgång till uppgifter eller material som har säkerhetsklassificerats och som har tillhandahållits eller utbytt enligt denna överenskommelse, görs en ändamålsenlig säkerhetsutredning innan de beviljas tillgång till sådana uppgifter och sådant material.

2. De fördragsslutande parterna säkerställer att tillgång till sådan säkerhetsklassificerad information som utbyts på basis av denna överenskommelse beviljas endast personer som behöver informationen för skötsel av sina uppgifter.

3. Syftet med säkerhetsutredningar skall vara att avgöra huruvida en person, med avseende på hans eller hennes lojalitet och tillförlitlighet, kan beviljas tillgång till säkerhetsklassificerad information.

4. Varje fördragsslutande part samarbetar på begäran med andra fördragsslutande parter vid genomförandet av säkerhetsutredningar.

Artikel 5

ESA:s generaldirektör säkerställer att de relevanta bestämmelserna i denna överenskommelse tillämpas vid rymdorganets huvudkontor, inrättningar och andra anläggningar.

Artikel 6

1. De fördragsslutande parterna undersöker alla fall där det konstateras eller misstänks att skyddet för säkerhetsklassificerad information som lämnats eller producerats inom ramen för denna överenskommelse har äventyrats eller förlorats.

2. Varje fördragsslutande part informerar, vid behov, snabbt och grundligt andra om alla detaljer som ansluter sig till fallet och om eventuella resultat av undersökningen samt om alla åtgärder som vidtagits för att förhindra en upprepning av dylikt röjande av information.

Artikel 7

I sådana fall där en representant för en medlemsstat eller ESA:s generaldirektör eller en medlem av ESA:s personal eller någon av dess experter är part i en rättsprocess som gäller obehörigt röjande av säkerhetsklassificerad information, är medlemsstaten, rådet och generaldirektören skyldiga att i enlighet med artiklarna XIV.2 och XXI.1 och 2 samt XXIV i bilaga 1 till ESA-konventionen avstå från immuniteten.

Artikel 8

Denna överenskommelse utgör inte på något sätt ett hinder för de fördragsslutande parterna att ingå andra avtal med anknytning till utbyte av sådan av säkerhetsklassificerad information som de producerat och som inte påverkar tillämpningsområdet för denna överenskommelse.

Artikel 9

1. Varje fördragsslutande part kan föreslå ändringar i denna överenskommelse.

2. Varje ändring av denna överenskommelse träder i kraft trettio dagar efter det att Frankrikes regering har mottagit ett meddelande om godkännande från alla fördragsslutande parter. Frankrikes regering informerar alla fördragsslutande parter om datumet för ikraftträdande av varje ändring.

Artikel 10

1. Denna överenskommelse är öppen för undertecknande av parterna i ESA-konventionen och den skall ratificeras, godtas eller godkännas. Ratifikations-, godtagande- eller godkännandeinstrumenten skall deponeras hos Frankrikes regering.

2. Överenskommelsen träder i kraft trettio dagar efter det att två signatärstater har deponerat sina ratifikations-, godtagande- eller godkännandeinstrument. I förhållande till varje annan signatärstat träder denna överenskommelse i kraft trettio dagar efter det att den staten har deponerat sitt ratifikations-, godtagande- eller godkännandeinstrument.

Artikel 11

1. Om någon ny part till ESA-konventionen skall tillträda denna överenskommelse skall det ske enligt artikel XXII i konventionen. För varje anslutande stat träder denna överenskommelse i kraft trettio dagar efter den dag då en sådan stat har deponerat sitt anslutningsinstrument.

2. Anslutningshandlingarna deponeras hos Frankrikes regering.

Artikel 12

1. Denna överenskommelse får sägas upp av en fördragsslutande part genom skriftlig underrättelse om uppsägning till depositarien som skall informera alla andra fördragsslutande parter om underrättelsen. Uppsägningen träder i kraft ett år efter det att depositarien har mottagit underrättelsen.

2. En fördragsslutande part som säger upp överenskommelsen skall vara bunden av skyldigheten att skydda och bevara den säkerhetsklassificerade information som den har fått tillgång till inom ramen för denna

överenskommelse. Detsamma gäller för en part i denna överenskommelse som säger upp ESA-konventionen i enlighet med artikel XXIV eller i fall att Europeiska rymdorganet upphör att existera i enlighet med artikel XXV av konventionen.

Artikel 13

Frankrikes regering skall underrätta ESA och alla signatärstater och anslutande stater om depositionen av varje ratifikations-, godtagande- och godkännande- eller uppsägningssinstrument.

Till bekräftelse härav har undertecknade, därtill vederbörligen bemyndigade av deras respektive regeringar, undertecknat denna överenskommelse.

Upprättad i Paris den 19 augusti 2002 på engelska och franska, vilka båda texter är lika giltiga, i ett enda exemplar, som skall deponeras hos Frankrikes regering. Bestyrkta kopior av överenskommelsen skall överlämnas av Frankrikes regering till varje signatärstat.

I Paris den 19 augusti 2002

Bilaga 2: **Överenskommelse mellan republiken Finlands regering och Tyska förbundsrepublikens regering om ömsesidigt skydd för säkerhetsklassificerad information**

Republiken Finlands regering och Tyska förbundsrepublikens regering, nedan ”de fördragsslutande parterna”, som

avser att säkerställa skyddet för säkerhetsklassificerad information som utbyts mellan republiken Finlands regering och Tyska förbundsrepublikens regering,

önskar få till stånd ett arrangemang för ömsesidigt skydd av säkerhetsklassificerad information som omfattar alla samarbetsavtal som ingås mellan de fördragsslutande parterna och avtal som inbegriper utbyte av säkerhetsklassificerad information,

har kommit överens om följande:

Artikel 1

Syfte

Syftet med denna överenskommelse är att skydda sådan information som av den ena fördragsslutande partens behöriga myndighet eller någon som verkar på uppdrag denna har säkerhetsklassificerat av skäl som rör någondera fördragsslutande partens allmänna intressen och som har förmedlats till den andra fördragsslutande parten via de behöriga myndigheterna antingen i samband med skötseln av de internationella relationerna, försvaret, polis- eller industriärenden eller i samband med sådana avtal som en enhet inom den ena fördragsslutande partens offentliga förvaltning har ingått med den andra fördragsslutande partens offentliga eller privata inrättningar.

Artikel 2

Definitioner

1) Med säkerhetsklassificerad information avses i denna överenskommelse

1. i Tyska förbundsrepublikens:

fakta, uppgifter eller underrättelser som

oavsett formen skall beläggas med sekretess i allmänintressets namn. Klassificering av informationen skall göras av en behörig myndighet eller någon som verkar på uppdrag av denna alltefter behovet av skydd,

2. i Finland:

fakta, uppgifter eller underrättelser som oavsett formen i allmänintressets namn skall beläggas med sekretess av skäl som anges i lagen. Informationen i fråga skall säkerhetsklassificeras av en behörig myndighet eller någon som verkar på uppdrag av denna allt efter behovet av skydd.

2) I denna överenskommelse definieras klassificeringsnivåerna på följande sätt:

1. I Tyska förbundsrepublikens används följande säkerhetsklassificering:

a) STRENG GEHEIM, om obehörigt röjande av informationen kan utgöra ett hot för existensen av Tyska förbundsrepublikens eller dess delstater eller för deras väsentliga intressen,

b) GEHEIM, om obehörigt röjande av informationen kan utgöra ett hot för Tyska förbundsrepublikens eller någon delstats säkerhet eller om den kan allvarligt skada deras intressen,

c) VS-VERTRAULICH, om obehörigt röjande av informationen kan skada Tyska förbundsrepublikens eller någon delstats intressen,

d) VS-NUR FÜR DEN DIENSTGEBRAUCH, om obehörigt röjande av informationen kan vara till nackdel för Tyska förbundsrepublikens eller någon delstats intressen.

2. I Finland används följande säkerhetsklassificering:

a) ERITTÄIN SALAINEN/YTTTERST HEMLIG, om obehörigt röjande av informationen kan orsaka särskilt påtaglig skada för försvaret, säkerheten, de internationella relationerna eller andra allmänna intressen,

b) SALAINEN/HEMLIG, om obehörigt

röjande av informationen kan orsaka väsentlig skada för försvaret, säkerheten, de internationella relationerna eller andra allmänna intressen,

c) LUOTTAMUKSELLINEN / KONFIDENTIELL, om obehörigt röjande av informationen kan skada försvaret, säkerheten, de internationella relationerna eller andra allmänna intressen,

d) KÄYTTÖ RAJOITETTU / BEGRÄNSAD TILLGÅNG, om obehörigt röjande av informationen kan skada det allmänna intresset eller begränsa myndigheternas möjligheter att agera.

Artikel 3

Överensstämmelse

De fördragsslutande parterna har beslutat att följande säkerhetsklasser motsvarar varandra och omfattas av denna överenskomst:

Tyska förbundsrepubliken

STRENG GEHEIM
GEHEIM
VS-VERTRAULICH
VS-NUR FÜR DEN DIENSTGEBRAUCH

Republiken Finland

ERITTÄIN SALAINEN/YTTERST HEM-
LIG
SALAINEN/HEMLIG
LUOTTAMUKSELLINEN / KONFIDEN-
TIELL
KÄYTTÖ RAJOITETTU/BEGRÄNSAD
TILLGÅNG

Artikel 4

Märkning

1) Den behöriga myndigheten i den mottagande staten eller den som verkar på uppdrag av denna skall förse den säkerhetsklassificerade information som har förmedlats med en säkerhetsklassificering som motsvarar den nationella klassificering som anges i artikel 3.

2) Den behöriga myndigheten i den mottagande staten eller den som verkar på uppdrag av denna skall förse också sådan klassificerad information som i den mottagande staten har producerats på basis av den information som förmedlats av den andra fördragsslutande parten med motsvarande säkerhetsklassificering. De kopior som tas i den mottagande staten skall också klassificeras på motsvarande sätt.

3) Den behöriga myndigheten i den stat som mottagit säkerhetsklassificerad information skall ändra klassificeringen eller upphäva den om den behöriga myndigheten i ursprungslandet begär det. Den behöriga myndigheten i ursprungslandet skall underrätta den andra fördragsslutande partens behöriga myndighet om sin avsikt sex veckor i förväg.

4) Den behöriga myndigheten i det land som mottagit säkerhetsklassificerad information kan be den behöriga myndigheten i ursprungslandet att ändra klassificeringen eller att upphäva den för den mottagna informationen i dess helhet eller för vissa särskilt angivna delar av den eller att ge en motivering till valet av en viss säkerhetsklass.

Artikel 5

Åtgärder på den nationella nivån

1) De fördragsslutande parterna skall inom ramen för sin egen lagstiftning vidta alla nödvändiga åtgärder för att skydda sådan säkerhetsklassificerad information som förmedlats på basis av denna överenskommelse eller som producerats i anslutning till ett klassificerat avtal som avses i artikel 6.1. De skall tillförsäkra informationen i fråga minst samma skydd som de ger åt sin egen information som hör till samma säkerhetsklass.

2) Artiklarna 5.4, artiklarna 6.2–6.5, artiklarna 7.1, 7.2, 7.4–7.6 och 7.8 samt artiklarna 8.1, 8.3 och 8.4 skall inte tillämpas på sådan information som klassificerats som VS-NUR FÜR DEN DIENSTGEBRAUCH / BEGRÄNSAD TILLGÅNG. Om inte annat bestäms i denna överenskommelse, skall sådan information som klassificerats som VS-NUR FÜR DEN DIENSTGEBRAUCH / BEGRÄNSAD TILLGÅNG hanteras enligt den mottagande statens nationella säkerhetsbe-

stämmelser som tillämpas på dylik information.

3) De fördragsslutande parterna får inte röja den säkerhetsklassificerade information som de mottagit för internationella organisationer eller för någon tjänsteman eller juridisk person i tredje land eller för en person som har sin hemvist i tredje land utan att den behöriga myndighet som fattat klassificeringsbeslutet i förväg har gett sitt skriftliga samtycke därtill. Den säkerhetsklassificerade informationen får användas endast för angivet ändamål. Speciellt bör noteras att tillgång till säkerhetsklassificerad information får beviljas endast personer som behöver ha tillgång till informationen för skötsel av sina uppgifter.

4) Tillgång till information som hör till säkerhetsklassen VS-VERTRAULICH/KONFIDENTIELL eller till en högre säkerhetsklass kan beviljas endast personer vars tillförlitlighet har fastställts (dvs. personer som varit föremål för en personlig säkerhetsutredning) och som har rätt att ha tillgång till informationen i fråga. En personlig säkerhetsutredning kan lämnas först efter en avslutad säkerhetsutredning som uppfyller minst lika stränga krav som en säkerhetsutredning som gäller tillgång till nationell säkerhetsklassificerad information i samma säkerhetsklass.

5) Tillgång till information som klassificerats om VS-NUR FÜR DEN DIENSTGEBRAUCH/BEGRÄNSAD TILLGÅNG kan beviljas personer som behöver ha tillgång till uppgifterna.

6) De fördragsslutande parterna skall inom sina respektive territorier säkerställa att de nödvändiga säkerhetsutredningarna utförs och att de uppfyller villkoren i denna överenskommelse.

Artikel 6

Säkerhetsklassificerade avtal

1) Med ett ”säkerhetsklassificerat avtal” avses i denna överenskommelse ett skriftligt avtal som är ömsesidigt bindande för de fördragsslutande parterna och på vilket den ena fördragsslutande partens lag tillämpas och vilket har ingåtts av en myndighet eller ett

företag inom den ena fördragsslutande partens territorium (uppdragsgivare) och vilket förpliktar en leverantör eller en underleverantör som har etablerat sig och har sitt registrerade säte inom den andra fördragsslutande partens territorium (uppdragstagare) att leverera varor eller tjänster och vilket innebär att uppdragstagaren behöver få tillgång till säkerhetsklassificerad information eller att uppdragstagarens personal i detta sammanhang kan komma att få tillgång till klassificerad information.

2) Innan ett avtal som tillhör säkerhetsklassen VS-VERTRAULICH / KONFIDENTIELL eller en högre säkerhetsklass ingås skall uppdragsgivaren genom sin egen behöriga myndighet få en säkerhetsutredning som gäller uppdragstagaren (säkerhetsutredning som gäller sammanslutning) och som har lämnats av uppdragstagarens behöriga myndighet för att försäkra sig om huruvida den potentiella uppdragstagaren är föremål för säkerhetskontroll av den behöriga myndigheten i sitt eget land och om uppdragstagaren har vidtagit nödvändiga säkerhetsåtgärder i syfte att inleda fullgörande av avtalet. I detta hänseende tillämpas följande förfarande:

1. Om uppdragstagaren inte ännu har vidtagit nödvändiga säkerhetsåtgärder, kan uppdragsgivarens behöriga myndighet samtidigt be uppdragstagarens behöriga myndighet att se till att uppdragstagaren vidtar nödvändiga säkerhetsåtgärder i enlighet med de nationella säkerhetsbestämmelserna och att sedan lämna en säkerhetsutredning som gäller sammanslutning till uppdragsgivarens behöriga myndighet.

2. En säkerhetsutredning som gäller sammanslutning måste också fås om och innan en potentiell uppdragstagare har blivit ombedd att lämna ett anbud som baserar sig på eller innehåller säkerhetsklassificerad information eller om eller innan klassificerad information skall överlämnas till en potentiell uppdragstagare som deltar i anbudsgivningen.

3. Begäran om en säkerhetsutredning som gäller sammanslutning i fråga om uppdragstagare som är verksamma inom den andra fördragsslutande partens territorium skall innehålla uppgifter om projektet liksom också om arten, omfattningen och

graden av säkerhetsklassificering hos den klassificerade information som förväntas bli överlämnad till uppdragstagaren eller producerad av denna.

4. Utöver uppdragstagarens fullständiga namn, postadress och namnet på den person som ansvarar för säkerheten, skall en säkerhetsutredning som gäller sammanslutning innehålla information särskilt om omfattningen och graden av nödvändiga säkerhetsåtgärder enligt klassificeringsnivån som uppdragstagaren har vidtagit på basis av de nationella säkerhetsbestämmelserna.

5. De fördragsslutande parternas behöriga myndigheter skall informera varandra om alla ändringar i de omständigheter som ingår i en säkerhetsutredning som gäller sammanslutning.

6. De fördragsslutande parternas behöriga myndigheter skall tillstålla varandra säkerhetsutredningar som gäller sammanslutningar vilka skall vara avfattade antingen på den mottagande behöriga myndighetens nationella språk eller på engelska.

7. Säkerhetsutredningar som gäller sammanslutning och skriftliga framställningar därom som adresserats till de fördragsslutande parternas behöriga myndigheter kan förmedlas skriftligen antingen genom diplomatkurir eller per post eller genom att anlita andra leveranstjänster, eller per telefax eller i form av andra elektroniska meddelanden.

3) De fördragsslutande parterna skall vidta alla nödvändiga åtgärder för att säkerställa att säkerhetsklassificerade avtal innehåller en klausul som ålägger uppdragstagaren att vidta nödvändiga åtgärder för att skydda säkerhetsklassificerad information i enlighet med det egna landets nationella säkerhetsbestämmelser.

4) Uppdragsgivarens behöriga myndighet skall ge uppdragstagaren en särskild förteckning (klassifikationsguide) över alla dokument som kräver klassificering, bestämma vilken säkerhetsklass som skall gälla och se till att förteckningen bifogas till klassificerade avtal. Uppdragsgivarens behöriga myndighet skall vidarebefordra förteckningen eller se till att förteckningen vidarebefordras till uppdragstagarens behöriga myndighet.

5) Uppdragsgivarens behöriga myndighet skall säkerställa att uppdragstagaren ges tillgång till säkerhetsklassificerad information först efter det att uppdragstagarens behöriga myndighet har lämnat den nödvändiga säkerhetsutredningen som gäller sammanslutning.

Artikel 7

Förmedling av säkerhetsklassificerad information

1) Information som säkerhetsklassificerats som STRENG GEHEIM/YTTERST HEM-LIG får förmedlas mellan de fördragsslutande parterna endast med diplomatpost.

2) Information som säkerhetsklassificerats som VS-VERTRAULICH/KONFIDENTIELL eller som GEHEIM/HEMLIG får förmedlas mellan de fördragsslutande parternas regeringar med diplomatpost eller via sådana kanaler som de båda fördragsslutande parternas behöriga myndigheter har godkänt, om inte något annat bestäms i denna överenskommelse.

3) Information som säkerhetsklassificerats som VS-NUR FÜR DEN DIENSTGEBRAUCH /BEGRÄNSAD TILLGÅNG får förmedlas mellan de fördragsslutande parterna i enlighet med den avsändande fördragsslutande partens nationella bestämmelser som kan tillåta att kommersiella leveranstjänster anlitas.

4) Vid vissa särskilt angivna projekt får de behöriga myndigheterna avtala - generellt eller i begränsad omfattning - att information som klassificerats som VS-VERTRAULICH / KONFIDENTIELL eller GEHEIM/HEMLIG på nedan angivna villkor får förmedlas från en regering till en annan via andra kanaler än med diplomatpost om anlitan av diplomatkanaler skulle kunna orsaka särskilda svårigheter med tanke på transporten eller fullgörande av avtalet. I dylika fall gäller att

1. budet skall vara behörigt att få tillgång till säkerhetsklassificerad information av motsvarande säkerhetsklass,

2. den sändande myndigheten skall behålla en förteckning över den säkerhets-

klassificerade information som förmedlats; en kopia av förteckningen skall överlämnas till mottagaren för att bli vidarebefordrad till den behöriga myndigheten,

3. material som innehåller säkerhetsklassificerad information skall förpackas i enlighet med de nationella bestämmelserna om transporter inom landet i fråga,

4. den säkerhetsklassificerade informationen får överlämnas endast mot mottagningsbevis,

5. budet skall bära med sig ett kuririntyg som utfärdats av antingen avsändarens eller mottagarens behöriga myndighet.

5) När stora mängder säkerhetsklassificerad information skall förmedlas, skall beslut om transportmedel, rutt och eskort (om sådan används) fattas gemensamt av de fördragsslutande parternas behöriga myndigheter.

6) I brådskande fall, t.ex. när anlitande av budtjänst inte skulle uppfylla uppställda krav, får information som klassificerats som VS-VERTRAULICH / KONFIDENTIELL, i samband med säkerhetsklassificerade avtal, också förmedlas med hjälp av kommersiella leveranstjänster. I dylika fall gäller följande villkor:

1. Den kommersiella leveranstjänsten skall vara etablerad inom någon av de fördragsslutande parternas territorium och ha ett säkerhetssystem för transport av värdeförsändelser, som också täcker distributionscentraler, och skall kunna t.ex. med hjälp av mottagningsbevis i en liggare eller ett kvittohäfte eller ett elektroniskt lokaliseringssystem/system för spårning bevisa att den kan hantera försändelser ansvarsfullt.

2. Den kommersiella leveranstjänsten skall förse avsändaren med bevis på att leverans ha skett antingen i form av ett undertecknat mottagningsbevis i ett kvittohäfte eller ha mottagarens kvittering på en fraktsedel som anger försändelsens registernummer.

3. Den kommersiella leveranstjänsten skall garantera att försändelsen levereras före en viss tidpunkt inom 24 timmar.

4. Den kommersiella leveranstjänsten får uppdras åt en representant eller en underleverantör att sköta förmedlingen och leveransen. Leveranstjänsten har dock alltid an-

svaret för att kriterierna enligt 1-3 punkten uppfylls.

5. Den kommersiella leveranstjänsten skall vara godkänd av de fördragsslutande parternas behöriga myndigheter.

7) Information som säkerhetsklassificerats som VS-NUR FÜR DEN DIENSTGEBRAUCH / BEGRÄNSAD TILLGÅNG får förmedlas per post eller av andra leveranstjänster till mottagare inom den andra fördragsslutande partens territorium, dock med beaktande av den sändande fördragsslutande partens nationella säkerhetsbestämmelser.

8) Information som tillhör säkerhetsklassen VS-VERTRAULICH/KONFIDENTIELL eller en högre säkerhetsklass får inte förmedlas elektroniskt okrypterad. Klassificerad information som tillhör någon av de nämnda säkerhetsklasserna får krypteras endast med hjälp av en krypteringsnyckel som har godkänts gemensamt av de fördragsslutande parternas behöriga myndigheter.

9) Information som tillhör säkerhetsklassen VS-NUR FÜR DEN DIENSTGEBRAUCH/BEGRÄNSAD TILLGÅNG får förmedlas elektroniskt eller dekrypteras med hjälp av kommersiella dekrypteringsnyckel som har godkänts gemensamt av de fördragsslutande parternas behöriga myndigheter. Klassificerad information i denna säkerhetsklass får förmedlas okrypterad endast under förutsättning att detta inte strider mot den sändande fördragsslutande partens nationella säkerhetsbestämmelser, att ingen godtagbar nyckel finns tillgänglig, att förmedling sker endast i fasta nätverk och att avsändaren och mottagaren har kommit överens om den föreslagna informationsförmedlingen i förväg.

Artikel 8

Besök

1) För att syftet med denna överenskommelse skall kunna uppnås skall de båda fördragsslutande parterna tillåta att den andra fördragsslutande partens representanter, civil- eller militärpersoner, eller uppdragstagares personal gör sådana besök hos den egna statens ämbetsverk och inrättningar och uppdragstagares verksamhetsutrymmen som in-

nebär att besökarna får tillgång till säkerhetsklassificerad information förutsatt att besökarna har varit föremål för en relevant personlig säkerhetsutredning och att de behöver få tillgång till uppgifterna.

2) Alla besökare skall uppfylla de säkerhetskrav som har uppställts av den av de fördragsslutande parterna som agerar värd. All säkerhetsklassificerad information som görs tillgänglig för eller överläts till besökare skall betraktas som sådan information som överlämnats till den fördragsslutande part som tagit initiativet till besöket och skall skyddas i enlighet med detta.

3) För besök hos den andra fördragsslutande partens statliga ämbetsverk och inrättningar i anslutning till klassificerad information utanför säkerhetsklassificerade avtal som förutsätter tillgång till information som tillhör säkerhetsklassen VS-VERTRAULICH / KONFIDENTIELL eller en högre säkerhetsklass krävs formella inbjudningar som skickas via regeringskanaler från en stat till en annan.

Dylika inbjudningar skall vara avfattade på värdstatens nationella språk eller på engelska och de skall innehålla följande information:

1. besökarens förnamn och efternamn, födelsedag och -ort, och hans/hennes passnummer eller ID-kortnummer,
2. besökarens nationalitet,
3. besökarens tjänstebetäckning, och namnet på den myndighet eller det verk som personen är anställd vid,
4. omfattningen av besökarens personliga säkerhetsutredning som anger hans/hennes rätt att få tillgång till säkerhetsklassificerad information,
5. syftet med besöket och den föreslagna tidpunkten för besöket,
6. namnen på de verk och anläggningar som skall besökas samt namnen på deras kontaktpersoner.

4) I fråga om besök hos den andra fördragsslutande partens statliga verk eller uppdragstagares verksamhetsutrymmen i anslutning till säkerhetsklassificerade avtal som förutsätter tillgång till information som klassificerats som VS-VERTRAULICH / KONFIDENTIELL eller GEHEIM/HEMLIG tillämpas följande förfarande:

1. Förberedelserna för besöken görs direkt

mellan den sändande anläggningen och den anläggning som skall besökas.

2. I fråga om besök skall också följande villkor uppfyllas:

a) Besöket skall ha ett officiellt syfte.

b) Säkerheten hos uppdragstagarens verksamhetsutrymmen som skall besökas har fastställts genom en relevant säkerhetsutredning som gäller sammanslutning.

c) Innan besökarna anländer skall den sändande anläggningens säkerhetsansvarige lämna en bekräftelse av besökarens personliga säkerhetsutredning direkt till den anläggning som skall besökas. För att besökarens identitet skall kunna fastställas skall denna ha med sig ett ID-kort eller pass för att visas upp för myndigheterna vid den anläggning som skall besökas.

d) De säkerhetsansvariga har följande skyldigheter:

aa) Den säkerhetsansvarige hos den sändande anläggningen skall hos sin behöriga myndighet försäkra sig om att alla uppdragstagares verksamhetsutrymmen som skall besökas har varit föremål för en relevant säkerhetsutredning som gäller sammanslutning.

bb) De säkerhetsansvariga hos både den sändande anläggningen och den anläggning som skall besökas skall vara överens om att besöket är motiverat.

e) De säkerhetsansvariga för de företags verksamhetsutrymmen eller, i relevanta fall för de statliga verk, som skall besökas skall försäkra sig om att alla besökare registreras genom att man i en liggare antecknar besökarnas namn, namnet på den organisation besökarna representerar, datumet då deras personliga säkerhetsutredning upphör att gälla, datumet/datumen för besöket och namnen på de personer hos vilka besök avläggs. Liggarna skall uppbevaras i minst fem års tid.

f) Världstatens behöriga myndighet har rätt att kräva att de enheter hos vilka besök avläggs i förväg anmäler besök som varar över 21 dagar. Myndigheten får sedan godkänna besöket men om några säkerhetsproblem uppstår skall den förhandla med besökarens behöriga myndighet.

5) Besök i anslutning till information som säkerhetsklassificerats som VS-NUR FÜR DEN DIENSTGEBRAUCH/BEGRÄNSAD TILLGÅNG skall ordnas direkt mellan den

sändande anläggningen och den anläggning som skall besökas utan några formaliteter.

Artikel 9

Förhandlingar

1) De fördragsslutande parternas behöriga myndigheter skall ta hänsyn till de bestämmelser om säkerhetsklassificerad information som tillämpas inom den andra fördragsslutande partens territorium.

2) För att kunna säkerställa ett nära samarbete mellan de fördragsslutande parterna för genomförande av överenskommelsen skall de behöriga myndigheterna förhandla med varandra när någon av de behöriga myndigheterna begär det.

3) De båda fördragsslutande parterna skall dessutom tillåta att den andra fördragsslutande partens behöriga myndigheter eller någon annan myndighet som parterna gemensamt har kommit överens om besöker dess territorium för att diskutera med dess myndigheter om de förfaranden som skall tillämpas och om de arrangemang som skall vidtas för att skydda säkerhetsklassificerad information som förmedlas mellan de fördragsslutande parterna. Bägge fördragsslutande parter skall hjälpa myndigheten i fråga när denna försäkras om att säkerhetsklassificerad information som utbyts mellan de fördragsslutande parterna är skyddad enligt artikel 5.1. De behöriga myndigheterna skall besluta om alla detaljer som rör besöken.

Artikel 10

Brott mot bestämmelserna om ömsesidigt skydd av säkerhetsklassificerad information

1) Om möjligheten till obehörigt röjande av säkerhetsklassificerad information inte kan uteslutas eller om obehörigt röjande misstänks eller har konstaterats, skall den andra fördragsslutande parten omedelbart underrättas.

2) Brott mot bestämmelserna om skyddet av säkerhetsklassificerad information skall undersökas och adekvata rättsliga åtgärder

vidtas av en behörig fördragsslutande parts behöriga myndigheter och domstolar i enlighet med dennas nationella lag. Den andra fördragsslutande parten skall på begäran bistå vid undersökningen och bli informerad om resultatet av den.

Artikel 11

Kostnader

En fördragsslutande part skall inte åläggas att ersätta de kostnader som orsakas av en annan fördragsslutande parts behöriga myndigheter vid tillämpning av överenskommelsen.

Artikel 12

Behöriga myndigheter

För att denna överenskommelse skall kunna genomföras skall de fördragsslutande parterna meddela varandra vilka myndigheter som är behöriga myndigheter.

Artikel 13

Slutbestämmelser

1) Denna överenskommelse träder i kraft femton dagar efter det att Tyska förbundsrepublikens regering har mottagit ett meddelande från Finlands regering om att de nationella åtgärder som behövs för överenskommelsens ikraftträdande har vidtagits.

2) När denna överenskommelse träder i kraft upphör det dokument av den 22 december 1997 som inbegriper en överenskommelse mellan Republiken Finlands försvarsministerium och Tyska förbundsrepublikens försvarsministerium om ömsesidigt skydd för sekretessbelagd försvarsinformation att gälla.

All säkerhetsklassificerad information som förmedlas innan denna överenskommelse träder i kraft är skyddad i enlighet med bestämmelserna i denna överenskommelse.

3) Överenskommelsen gäller på obestämd tid.

4) Ändringar kan göras i överenskommelsen efter det att de båda fördragsslutande parterna skriftligen gett sitt ömsesidiga samtycke därtill. Bägge fördragsslutande parter får när som helst begära ändring av överenskommelsen. Om den ena av de fördragsslutande parterna begär det, skall de fördragsslutande parterna inleda förhandlingar i syfte att ändra överenskommelsen.

5) Varje fördragsslutande part kan säga upp överenskommelsen med iakttagande av sex månaders uppsägningstid genom att skriftligen via diplomatkanaler underrätta den andra fördragsslutande parten om detta. Om uppsägning sker, skall den säkerhetsklassificerade information som förmedlats eller information som producerats av en uppdragstagare på basis av denna överenskommelse också i fortsättningen hanteras i enlighet med bestämmelserna i denna överenskommelse så

länge detta är motiverat med tanke på säkerhetsklassificeringen.

6) Den av de fördragsslutande parterna inom vars territorium överenskommelsen träffas vidtar åtgärder för registrering av överenskommelsen hos Förenta nationernas sekretariat enligt artikel 102 i Förenta nationernas stadga omedelbart efter det att överenskommelsen har trätt i kraft. Den andra fördragsslutande parten skall underrättas om registreringen och om FN:s registreringsnummer så snart registreringen har bekräftats av sekretariatet.

Upprättad i Helsingfors den 25 februari 2004

i två original på tyska, finska och engelska språken, vilka alla äger lika giltighet. Om det uppstår oklarheter vid tolkningen, skall den engelska texten ha företräde.

För Republiken Finlands regering

Johannes Koskinen

För Tyska förbundsrepublikens regering

Hanns Schumacher