17.3.2023

Regeringens proposition till riksdagen om godkännande och sättande i kraft av avtalet mellan parterna i nordatlantiska fördraget om informationssäkerhet och av säkerhetsbestämmelserna samt om uppsägning av det administrativa arrangemanget för skydd av säkerhetsklassificerad information som utbyts mellan Finland och Nordatlantiska fördragsorganisationen och av överenskommelsen med Nordatlantiska fördragsorganisationen om informationssäkerhet

PROPOSITIONENS HUVUDSAKLIGA INNEHÅLL

I denna proposition föreslås det att riksdagen godkänner ett avtal mellan parterna i nordatlantiska fördraget om informationssäkerhet samt säkerhetsbestämmelser och att riksdagen antar en lag om sättande i kraft av de bestämmelser i avtalet och i säkerhetsbestämmelserna som hör till området för lagstiftningen. I propositionen föreslås det även att riksdagen ger sitt samtycke till att Finland säger upp det administrativa arrangemanget för skydd av säkerhetsklassificerad information som utbyts mellan Finland och Nordatlantiska fördragsorganisationen samt överenskommelsen med Nordatlantiska fördragsorganisationen om informationssäkerhet.

Avtalet mellan parterna i nordatlantiska fördraget om informationssäkerhet är en del av Nordatlantiska fördragsorganisationens (Nato) rättsligt bindande avtalsram, som de nya medlemsländer som ansluter sig till nordatlantiska fördraget förutsätts förbinda sig till. Avtalet innehåller sådana bestämmelser om ömsesidigt skyddande och säkrande av säkerhetsklassificerad information som tillämpas mellan parterna i nordatlantiska fördraget. Detta multilaterala avtal ersätter de bilaterala informationssäkerhetsarrangemangen mellan Finland och Nordatlantiska fördragsorganisationen.

Avtalet mellan parterna i nordatlantiska fördraget om informationssäkerhet ingicks i Bryssel den 6 mars 1997 och trädde i kraft internationellt den 16 augusti 1998. Avtalet träder i kraft för Finlands del trettio dagar efter den dag då Finland deponerar sitt anslutningsinstrument för avtalet hos Amerikas förenta staters regering. Lagen om sättande i kraft av avtalet och av säkerhetsbestämmelserna avses träda i kraft samtidigt som avtalet träder i kraft för Finlands del, vid en tidpunkt som föreskrivs genom förordning av statsrådet. Lagen om upphävande av lagen om sättande i kraft av de bestämmelser som hör till området för lagstiftningen i det administrativa arrangemanget för skydd av säkerhetsklassificerad information som utbyts mellan Finland och Nordatlantiska fördragsorganisationen samt i överenskommelsen med Nordatlantiska fördragsorganisationen om informationssäkerhet avses träda i kraft samtidigt som uppsägningen av dessa fördrag träder i kraft, vid en tidpunkt som föreskrivs genom förordning av statsrådet.

INNEHÅLL

MOTIVERING

1 Bakgrund och beredning

1.1 Avtalet mellan parterna i nordatlantiska fördraget om informationssäkerhet

I det år 1997 ingångna avtalet mellan parterna i nordatlantiska fördraget om informationssäkerhet (nedan även *informationssäkerhetsavtalet*) konstateras det att effektivt politiskt samråd, samarbete och planering i försvarsfrågor i syfte att uppnå målen för fördraget förutsätter utbyte av säkerhetsklassificerad information mellan parterna. För utbyte av information behövs det bestämmelser om ömsesidigt skyddande och säkrande av säkerhetsklassificerad information. Syftet med avtalet är att skapa en allmän ram för säkerhetskrav och säkerhetsförfaranden.

Med informationssäkerhet avses alla förfaranden som skyddar informationsinnehåll gentemot utomstående (informationens konfidentialitet), informationens oföränderlighet (riktighet) samt informationens tillgänglighet. För att trygga informationssäkerheten används olika metoder. De vanligaste är säkerställande av personalens pålitlighet och lokalernas säkerhet, sekretessbestämmelser och det att rätten att använda informationen begränsas till enbart överenskomna ändamål samt olika typer av procedurkrav för hantering och överföring av information. Informationssäkerhetskraven omfattar informationens hela livscykel, inbegripet förvärvande, bearbetning, användning, överlåtelse, arkivering och förstöring.

I informationssäkerhetsavtalet definieras Natos och medlemsstaternas säkerhetsklassificerade information på vilken avtalet tillämpas. Avtalet utgår från att parterna ska bevara informationens säkerhetsklassificering och göra sitt yttersta för att säkra informationen. Informationen ska inte lämnas ut till tredje parter utan samtycke från den part som informationen härrör från. Varje part ska inrätta en nationell säkerhetsmyndighet för att genomföra avtalet. Enligt avtalet ska de som behandlar information i säkerhetsklassen CONFIDENTIAL eller högre genomgå en relevant säkerhetsutredning.

Enligt avtalet ska parterna utarbeta säkerhetskrav, som ska säkerställa en gemensam skyddsnivå för säkerhetsklassificerad information. Kraven i Natos säkerhetsbestämmelser gäller personalsäkerhet, datamaterialsäkerhet, lokalsäkerhet, säkerhet i kommunikations- och informationssystem samt industrisäkerhet.

Avtalet från 1997 ersatte det säkerhetsavtal som parterna ingått 1952. Alla nuvarande medlemsstater i Nordatlantiska fördragsorganisationen är parter i informationssäkerhetsavtalet.

1.2 Det administrativa arrangemanget för skydd av säkerhetsklassificerad information som utbyts mellan Finland och Nordatlantiska fördragsorganisationen samt överenskommelsen med Nordatlantiska fördragsorganisationen om informationssäkerhet

Överenskommelsen mellan Finland och Nordatlantiska fördragsorganisationen om informationssäkerhet (*Security Agreement between Finland and the North Atlantic Treaty Organization*) undertecknades den 22 september 1994, efter att Finland anslutit sig till Natos program för partnerskap för fred (*Partnership for Peace, PfP*). I överenskommelsen avtalade man om utbyte och skydd av säkerhetsklassificerad information.

Genom överenskommelsen mellan Finland och Nato förband sig Finland att klassificera och skydda det material som erhålls av Nato inom ramen för programmet för partnerskap för fred och att göra säkerhetsutredningar av dem som har tillgång till skyddat material. Till överenskommelsen hade det fogats en redogörelse för den säkerhetsklassificering av handlingar som

Nato tillämpar och för vissa administrativa arrangemang som behöver vidtas för genomförandet av överenskommelsen.

Samtidigt undertecknades också en uppförandekod (*Code of Conduct*) som gällde användningen av Natos lokaler och som hänförde sig till det att finländska representanter i ökad omfattning började röra sig i Natos lokaler. Genom att underteckna uppförandekoden förband sig Finland till att inte använda Natos lokaler för osaklig verksamhet. Genom utrikesministeriets beslut av den 13 september 1994 godkändes dessutom två handlingar av administrativ natur i anslutning till överenskommelsen om informationssäkerhet (minimistandarder som gäller säkerhetsklassificerad information samt ett verkställighetsarrangemang). Genom beslutet utsågs också utrikesministeriet till den förvaltningsmyndighet med ansvar för informationssäkerhets- och dokumentsäkerhetsfrågor som krävdes enligt överenskommelsen. I föredragningspromemorian till beslutet anges förvaltningsmyndighetens uppgifter genom hänvisningar till uppgifterna för den säkerhetsmyndighet som avses i överenskommelsen och till centralregistret (*Central Registry).*

Det ansågs att överenskommelsen i enlighet med den då gällande konstitutionen kunde ingås som ett så kallat internationellt förvaltningsavtal mellan myndigheterna, eftersom en överenskommelse gällande dokumentsäkerhet karakteriserades som en handling av administrativ natur som hänför sig till det praktiska samarbetet. Överenskommelsen och dess bilagor ansågs inte strida mot den finska lagstiftningen. Ett beslut om undertecknande av överenskommelsen och uppförandekoden fattades därför vid utrikesministeriet efter en remissbehandling, och överenskommelsen undertecknades av Finlands representant i Nato.

År 2004 stiftades lagen om internationella förpliktelser som gäller informationssäkerhet (588/2004), vilken ska tillämpas på särskilt känsligt informationsmaterial. Med särskilt känsligt informationsmaterial avses till en finsk myndighet lämnade handlingar och material, vilka avsändaren i enlighet med en internationell överenskommelse eller någon annan internationell förpliktelse som är bindande för Finland har försett med en anteckning om säkerhetsklass. Lagen kan tillämpas endast om den internationella överenskommelsen har satts i kraft i Finland på det sätt som grundlagen kräver eller om det är fråga om en internationell förpliktelse som annars är bindande för Finland.

Statsrådets allmänna sammanträde tillsatte 2012 en delegation för förhandlingar om ett administrativt arrangemang som skulle komplettera överenskommelsen om informationssäkerhet från 1994 i syfte att uppdatera överenskommelsen så att bestämmelserna i lagen om internationella förpliktelser som gäller informationssäkerhet samt gällande säkerhetsföreskrifter beaktas. I enlighet med detta förhandlade parterna under våren 2012 fram ett arrangemang som kompletterade överenskommelsen. Det administrativa arrangemanget undertecknades i Helsingfors den 3 juli 2012. Det innehåller bland annat bestämmelser om märkning av säkerhetsklassificerad information, skydd av och tillgång till informationen, detaljer i säkerhetskraven samt säkerhetskontroller. I samband med att det administrativa arrangemanget godkändes nationellt sattes också Finlands och Natos överenskommelse om informationssäkerhet från 1994 i kraft nationellt (FördrS 7 och 8/2013). Lagen om sättande i kraft av de bestämmelser som hör till området för lagstiftningen i det administrativa arrangemanget och i överenskommelsen om informationssäkerhet från 1994 (945/2012) utfärdades den 21 december 2012 och trädde i kraft den 1 februari 2013. När Finland ansluter sig till Natos multilaterala informationssäkerhetsavtal är avsikten att dessa bilaterala informationssäkerhetsarrangemang sägs upp och att lagen om sättande i kraft av dem upphävs.

1.3 Beredning

Beredningen av avtalet

Den 17 maj 2022 beslutade republikens president på framställning av statsrådet att Finland skulle meddela Nordatlantiska fördragsorganisationen om Finlands intresse av att föra samtal om att ansluta sig till Nato. Samma dag utnämnde republikens president även Finlands delegation för anslutningssamtalen. Finland anmälde sitt intresse till Natos generalsekreterare genom utrikesministerns brev som överlämnades i Bryssel den 18 maj 2022. Natomedlemsstaternas stats- och regeringschefer bjöd in Finland till anslutningssamtal den 29 juni 2022 i samband med toppmötet i Madrid.

Anslutningssamtalen mellan Finland och Nato fördes vid Natos högkvarter i Bryssel den 4 juli 2022. Anslutningssamtalen fördes om fem delområden: 1) politiska frågor och politiken för bekämpning av terrorism, 2) försvarsfrågor och militära frågor, 3) resursfrågor, 4) informationssäkerhetsfrågor och 5) juridiska frågor. Enligt anslutningssamtalen ska Finland ansluta sig till följande sex Natofördrag inom 12 månader från deponeringen av Finlands anslutningsinstrument för nordatlantiska fördraget: avtalet mellan parterna i nordatlantiska fördraget om status för deras styrkor (Nato SOFA), protokollet om status för de internationella militära högkvarter som inrättats enligt nordatlantiska fördraget (Parisprotokollet), avtalet om överföring av teknisk information för försvarsändamål, avtalet om ömsesidigt sekretesskydd för patentsökta försvarsrelaterade uppfinningar, avtalet mellan parterna i nordatlantiska fördraget om informationssäkerhet samt avtalet mellan parterna i nordatlantiska fördraget om samarbete avseende nukleär information.

Efter anslutningssamtalen beslutade republikens president den 4 juli 2022 enligt statsrådets förslag till avgörande att Finland skulle lämna Nordatlantiska fördragsorganisationen en avsiktsförklaring om anslutning till nordatlantiska fördraget. Avsiktsförklaringen lämnades till Nato den 5 juli 2022, och parterna i nordatlantiska fördraget undertecknade Finlands anslutningsprotokoll samma dag.

Beredningen på nationell nivå

Vid statsrådets allmänna sammanträde den 15 september 2022 tillsattes en koordineringsgrupp med underlydande expertgrupper för beredningen av en regeringsproposition om godkännande av nordatlantiska fördraget. Regeringens proposition till riksdagen om godkännande och sättande i kraft av nordatlantiska fördraget och avtalet om status för Nordatlantiska fördragsorganisationen, nationella representanter och organisationens internationella personal (RP 315/2022 rd) lämnades till riksdagen den 5 december 2022.

Man beslutade att de ytterligare sex fördrag som Finland ska ansluta sig till bereds och lämnas till riksdagen i form av separata regeringspropositioner. Den 5 december 2022 tillsatte utrikesministeriet en arbetsgrupp för beredningen av regeringens proposition om godkännande av Natos informationssäkerhetsavtal. Arbetsgruppen bestod av företrädare för utrikesministeriet, försvarsministeriet, justitieministeriet, Skyddspolisen samt Transport- och kommunikationsverket. Arbetsgruppen sammanträdde totalt 11 gånger. Arbetsgruppen hörde under beredningen republikens presidents kansli samt ministerier som inte var företrädda i arbetsgruppen. Statsrådets kansli, finansministeriet, arbets- och näringsministeriet, social- och hälsovårdsministeriet samt jord- och skogsbruksministeriet deltog.

Arbetsgruppen färdigställde sitt betänkande i form av en regeringsproposition den 22 mars 2023.

Utlåtanden om utkastet till proposition inhämtades av bland annat ministerierna, andra myndigheter, företrädare för näringslivet samt organisationer, sammanlagt xx instanser, mellan den 24 mars och 21 april 2023 i tjänsten utlåtande.fi. Utlåtandena och ett sammandrag av utlåtandena finns på statsrådets projektsida under numret UM001:00/2023.

2 Gällande lagstiftning och bedömning av den

2.1 Lagen om internationella förpliktelser som gäller informationssäkerhet

Lagens allmänna tillämpningsområde

Lagen om internationella förpliktelser som gäller informationssäkerhet (588/2004) tillämpas på särskilt känsligt informationsmaterial. Med det avses sådana sekretessbelagda handlingar och material samt sådan information som kan fås ur dem samt sådana handlingar och material som producerats utifrån dessa handlingar och material samt denna information och som har säkerhetsklassificerats enligt en internationell förpliktelse som gäller informationssäkerhet. Bestämmanderätten över särskilt känsligt informationsmaterial kvarstår även efter utlämnandet hos den stat, internationella organisation eller det organ som lämnat ut materialet. Lagen kan endast tillämpas om den internationella överenskommelsen har satts i kraft i Finland på det sätt som grundlagen kräver eller om det är fråga om en internationell förpliktelse som gäller informationssäkerhet som annars är bindande för Finland.

Till kategorin särskilt känsligt informationsmaterial som omfattas av lagens tillämpningsområde hänförs ytterligare handlingar som har upprättats av en finsk myndighet eller av en näringsidkare som omfattas av lagens tillämpningsområde, av vilka framgår information som ingår i särskilt känsligt informationsmaterial som har sänts till Finland eller information som kan hämtas ur sådant material. Lagen tillämpas inte endast på hemlighållande eller klassificering av handlingar och delar av handlingar som innehåller nationell information från Finland.

Lagen innehåller bestämmelser om utfärdande av intyg över säkerhetsutredning av person (*Personnel Security Clearance, PSC*) och säkerhetsutredning av företag (*Facility Security Clearance, FSC*). För utfärdandet av intyg och prövningen i anslutning till detta ska den myndighet som gjort säkerhetsutredningen av person eller företag trots sekretessbestämmelserna lämna den nationella säkerhetsmyndigheten information om alla sådana omständigheter som vid utredningen framkommit i fråga om den person eller det företag som utredningen gäller (11 § 1 mom. och 12 § 1 mom.).

Säkerhetsutredningslagen (726/2014) tillämpas i fråga om bedömning av huruvida ett intyg ska utfärdas samt om giltighet för och återkallelse av ett intyg (11 § 2 mom. och 12 § 2 mom. i lagen om internationella förpliktelser som gäller informationssäkerhet). Om den nationella säkerhetsmyndigheten vägrar att utfärda ett intyg över säkerhetsutredning av person eller företag, ska den meddela skälen för detta i ett skriftligt beslut som ges till den som ansökt om utredningen och den som utredningen gäller (11 § 3 mom. och 12 § 3 mom. i lagen om internationella förpliktelser som gäller informationssäkerhet). Bestämmelser om ändringssökande finns i den lagens 20 a §.

Lagen om internationella förpliktelser som gäller informationssäkerhet har ändrats sex gånger sedan den stiftades. Lagen tillhandahåller alltjämt en lämplig lagstiftningsram också för genom-

förandet av Natos informationssäkerhetsavtal i Finland. Informationssäkerhetsavtalet förutsätter inga ändringar i lagen, men i ljuset av den 20-åriga tillämpningspraxisen för lagen är det nyttigt att framöver bedöma eventuella behov av ändringar.

Lagens förhållande till lagstiftningen om offentlighet och informationshantering

Enligt 12 § om yttrandefrihet och offentlighet i grundlagen är handlingar och upptagningar som innehas av en myndighet offentliga, om inte offentligheten av tvingande skäl särskilt har begränsats genom lag, och var och en har rätt att ta del av offentliga handlingar och upptagningar. Offentlighetsprincipen förstärktes i Finlands statsförfattning i samband med reformen av de grundläggande fri - och rättigheterna när det till den dåvarande regeringsformen fogades en bestämmelse om rätten att ta del av handlingar och upptagningar som innehas av en myndighet (RP 309/1993 rd, s. 62 och GrUB 25/1994 rd, s. 9). Den offentlighetsprincip som härleds ur 12 § 2 mom. i grundlagen framgår av 1 § i lagen om offentlighet i myndigheternas verksamhet (621/1999, nedan *offentlighetslagen*). Enligt 1 § 1 mom. i offentlighetslagen är myndighetshandlingar offentliga, om inte något annat föreskrivs särskilt i offentlighetslagen eller i någon annan lag. Enligt förarbetena till offentlighetslagen stärker bestämmelsen offentlighetsprincipen som den centrala principen för den offentliga förvaltningen i Finland. Syftet med paragrafen är också att betona att offentlighetsprincipen är huvudregeln, från vilken man kan avvika endast genom lag.

På Natos handlingar tillämpas i princip inte offentlighetsprincipen utifrån organisationens egna bestämmelser eller praxis, och i fråga om Nato har det inte föreskrivits om en allmän principiell rätt att få information om organisationens handlingar.

På handlingar som innehas av finska myndigheter tillämpas offentlighetslagen, om inte något annat föreskrivs i lag. Enligt offentlighetslagen är myndighetshandlingar sådana handlingar som har upprättats vid skötseln av uppgifter inom myndighetens verksamhetsområde, som har tillställts myndigheten och som innehas av myndigheten (5 §). Med andra ord är både handlingar som myndigheten själv upprättat och som gäller Natosamarbetet och andra handlingar som myndigheten innehar och som fåtts inom ramen för Natosamarbetet sådana myndighetshandlingar som avses i offentlighetslagen. På Natos säkerhetsklassificerade handlingar tillämpas specialbestämmelsen om absolut sekretess enligt lagen om internationella förpliktelser som gäller informationssäkerhet, och dessa handlingar är inte föremål för sådan bedömning av klausuler om skaderekvisit i fråga om sekretess som avses i offentlighetslagen. Natos säkerhetsklassificerade handlingar ska således hemlighållas, om inte något annat följer av de överenskommelser eller regler som gäller dem.

Handlingar som upprättats av en myndighet omfattas av rätten att få uppgifter i enlighet med offentlighetslagen när den tidpunkt som föreskrivs i 6 § i offentlighetslagen har nåtts vid behandlingen av ärendet. På motsvarande sätt börjar offentligheten för handlingar som har lämnats in till en myndighet från den tidpunkt då de har kommit in till myndigheten (7 §). Efter nämnda tidpunkter ska uppgifter ur en handling lämnas ut, om inte något annat följer av sekretessbestämmelserna eller andra bestämmelser om begränsning av rätten att ta del av en handling. Myndigheten har prövningsrätt när det gäller att lämna ut uppgifter ur en till sitt innehåll offentlig handling före den tidpunkt handlingen blir offentlig (9 §).

Enligt Natos säkerhetsstrategi är sådan Natoinformation offentlig Natoinformation som inte har säkerhetsklassificerats och som offentliggörs av den organisation eller byrå inom Nato som ansvarar för ärendet. Information som är avsedd för Natos interna bruk och som inte är säkerhetsklassificerad anges med NATO UNCLASSIFIED (NU). Sådan information får enligt säkerhetsstrategin lämnas ut endast till personer som behöver informationen (need-to-know). När en

handling innehas av en finsk myndighet bedöms handlingens offentlighet med stöd av offentlighetslagen.

Utgångspunkten enligt offentlighetslagen är att sekretessen för en handling grundar sig på de sekretessgrunder som föreskrivs i lag och att uppgifter ur en offentlig handling får lämnas ut utan att den som begär uppgifterna behöver den begärda informationen. Rätten att få uppgifter kan enligt grundlagen begränsas endast för att trygga sådana i lag angivna intressen som anses nödvändiga. I 24 § i offentlighetslagen finns allmänna bestämmelser om skyldighet att iaktta handlingssekretess. Den viktigaste sekretessbestämmelsen med tanke på fastställandet av offentligheten för handlingar som anknyter till Natosamarbetet är 24 § 1 mom. 2 punkten. De handlingar som avses i bestämmelsen är sekretessbelagda om utlämnandet av uppgifter ur dem skulle medföra skada eller olägenhet för Finlands internationella förhållanden eller förutsättningar att delta i det internationella samarbetet. Med stöd av bestämmelsen kan till exempel handlingar som upprättats av ett internationellt samfund eller organ vara sekretessbelagda, om de är sekretessbelagda hos samfundet eller organet (RP 30/1998 rd). Andra sekretessbestämmelser som kan komma i fråga är 24 § 1 mom. 1 och 7–10 punkten i offentlighetslagen.

I lagen om internationella förpliktelser som gäller informationssäkerhet finns det bestämmelser som avviker från bestämmelserna om nationella handlingars informationssäkerhet. I 3 § 1 mom. finns dock en allmän hänvisningsbestämmelse till offentlighetslagen och lagen om informationshantering inom den offentliga förvaltningen (906/2019, nedan *informationshanteringslagen*). Till de delar finska myndigheters handlingar innehåller annan information om internationellt samarbete än sådan som omfattas av internationella förpliktelser om informationssäkerhet ska lagen om internationella förpliktelser som gäller informationssäkerhet tillämpas på den informationen. I övrigt tillämpas offentlighetslagen och informationshanteringslagen och de bestämmelser som utfärdats med stöd av dem. Som det har konstaterats föreskrivs det i offentlighetslagen bland annat om rätten att ta del av myndigheternas offentliga handlingar samt om tystnadsplikt för den som är anställd hos en myndighet och handlingssekretess. I informationshanteringslagen finns bestämmelser om informationshantering i fråga om myndigheternas informationsmaterial och användning av informationssystem. I 4 kap. i informationshanteringslagen finns det, efterliknande internationella förpliktelser som gäller informationssäkerhet, bestämmelser om allmänna informationssäkerhetsåtgärder i anslutning till identifiering av uppgifter som förutsätter särskild tillförlitlighet (12 §), informationssäkerhet i fråga om informationsmaterial och informationssystem (13 §), informationsöverföring i datanät (14 §), tryggande av säkerheten i fråga om informationsmaterial (15 §), kontroll av användarrättigheter för informationssystem (16 §), insamling av logginformation (17 §) och säkerhetsklassificering av handlingar inom statsförvaltningen (18 §).

Enligt 3 § 2 mom. i lagen om internationella förpliktelser som gäller informationssäkerhet ska en på offentlighetslagen eller på någon annan lag baserad begäran om att få uppgifter ur särskilt känsligt informationsmaterial handläggas och avgöras av den myndighet till vilken informationsmaterialet har sänts eller som ska behandla ärendet i dess helhet. I 6 § 1 mom. i den lagen föreskrivs om en särskild sekretessgrund, enligt vilken särskilt känsligt informationsmaterial ska sekretessbeläggas, om inte annat följer av en internationell förpliktelse som gäller informationssäkerhet. Enligt 7 § 2 mom. i den lagen gäller 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 utför uppdraget samt i fråga om förbud mot utnyttjande i samband därmed vad som föreskrivs i lagen om offentlighet i myndigheternas verksamhet. Enligt 8 § 1 mom. i den lagen ska särskilt känsligt informationsmaterial oberoende av vad som föreskrivs i informationshanteringslagen eller med stöd av den förses med en sådan anteckning om säkerhetsklass som anges i en internationell förpliktelse som gäller informationssäkerhet och som anger vilka säkerhetskrav som ska iakttas vid hanteringen av materialet.

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

Dessutom föreskrivs det i 30 § i offentlighetslagen att en myndighet kan lämna ut uppgifter ur en sekretessbelagd handling till en utländsk myndighet eller ett internationellt organ, om samarbetet mellan den utländska och den finska myndigheten regleras i en för Finland bindande internationell överenskommelse eller föreskrivs i en rättsakt som är bindande för Finland och om uppgifter ur handlingen enligt den lagen kan lämnas ut till den finska myndighet som bedriver samarbetet. Enligt 17 § i lagen om internationella förpliktelser som gäller informationssäkerhet har finska myndigheter på motsvarande sätt rätt att till en annan avtalspart lämna ut handlingar och information som är nödvändiga för fullgörandet av en internationell förpliktelse som gäller informationssäkerhet, trots vad som i finsk lagstiftning föreskrivs om sekretessbeläggning av handlingar och uppgifter.

Tillämpning av lagen på näringsidkare

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

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

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

Verkställande myndigheter

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

Sekretessbeläggning och reglering av informationsanvändningen

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

Säkerhetsklassificering och skyddsåtgärder

I lagen om internationella förpliktelser som gäller informationssäkerhet föreskrivs om skyldigheten att förse särskilt känsligt informationsmaterial med anteckning om säkerhetsklass. Särskilt känsligt informationsmaterial ska förses med en sådan anteckning om säkerhetsklass som anger vilka säkerhetskrav som ska iakttas vid hanteringen av materialet (8 §). Ju högre materialets säkerhetsklass är, desto strängare säkerhetsåtgärder krävs det. Lagen innehåller en allmän förpliktelse att tillämpa de bestämmelser om hantering av informationsmaterialet som materialets säkerhetsklass förutsätter samt ett bemyndigande att föreskriva om säkerhetsåtgärder vid hantering av särskilt känsligt informationsmaterial som motsvarar de olika säkerhetsklasserna genom förordning av statsrådet (9 §). I 4 § i statsrådets förordning om säkerhetsklassificering av handlingar inom statsförvaltningen (1101/2019, nedan *säkerhetsklassificeringsförordningen),* finns det bestämmelser om säkerhetsklassificeringens motsvarighet vid tillgodoseende av internationella förpliktelser som gäller informationssäkerheten. Bestämmelsen tillämpas om inte något annat följer av en internationell förpliktelse som gäller informationssäkerhet.

Enligt 10 § i lagen om internationella förpliktelser som gäller informationssäkerhet ska särskilt känsligt informationsmaterial förvaras i utrymmen där det är möjligt att skydda handlingarna och materialen samt informationen i dem i enlighet med en internationell förpliktelse som gäller informationssäkerhet. Bestämmelser om kraven på säkerheten i sådana lokaler och utrymmen finns i 9 och 10 § i säkerhetsklassificeringsförordningen.

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

Informationssystemsäkerhet

Transport- och kommunikationsverket är enligt 4 § i lagen om internationella förpliktelser som gäller informationssäkerhet sakkunnig vid den nationella säkerhetsmyndigheten i frågor som gäller informationssäkerheten i informationssystem och datakommunikation och svarar bland annat för de bedömningar och uppgifter som gäller godkännande av informationssystem (ackreditering) som internationella förpliktelser som gäller informationssäkerhet förutsätter. Bestämmelser om förfarandet vid bedömning av informationssäkerheten i myndigheternas informationssystem och om Transport- och kommunikationsverkets uppgift att bedöma informationssäkerheten finns i lagen om bedömning av informationssäkerheten i myndigheternas informationssystem och datakommunikation (1406/2011, nedan *bedömningslagen*). Vid bedömningen av informationssystemen kan myndigheterna också anlita sådana av Transport- och kommunikationsverket godkända bedömningsorgan som avses i lagen om bedömningsorgan för informationssäkerhet (1405/2011). Tills vidare har bedömningsorganen inte godkänts att utföra bedömningar av informationssystem där EU:s eller Natos säkerhetsklassificerade information behandlas. Bestämmelser om bedömning av företags informationssystem som en del av säkerhetsutredningen av företag finns i säkerhetsutredningslagen.

2.2 Säkerhetsutredningslagen

Lagens syfte och tillämpningsområde

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

I lagen finns bestämmelser om det förfarande som ska iakttas vid genomförande av säkerhetsutredningar av person och av företag. Lagen innehåller bestämmelser om förutsättningarna för säkerhetsutredningar och om vilka uppgifter som ska användas för en säkerhetsutredning, samtycke av och rätt till information för den som utredningen gäller, uppgiftsskyldigheten för den som ansöker om säkerhetsutredning och den som utredningen gäller, giltigheten av säkerhetsutredningar och intyg över säkerhetsutredningar samt om återkallelse av intyg samt om samkörning av personregister för att kontrollera att den som utredningen gäller är oförvitlig och tillförlitlig och om de åtgärder som ska genomföras med anledning av samkörningen (2 §). En säkerhetsutredning kan göras endast om den som utredningen gäller på förhand har gett sitt skriftliga samtycke till detta (5 §).

Personalsäkerhet

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

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

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

I lagen finns också en uttömmande förteckning över de register som får användas vid förfarandet med säkerhetsutredning. Vid säkerhetsutredningar får också användas uppgifter i vissa register som förs av en myndighet i en annan stat (25 §).

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

Företagssäkerhet

Med säkerhetsutredning av företag avses enligt 3 § 1 mom. 2 punkten i säkerhetsutredningslagen en utredning som görs i enlighet med säkerhetsutredningslagen för att bedöma ett företags och dess ansvarspersoners tillförlitlighet samt företagets informationssäkerhetsnivå och förmåga att sköta åtaganden. En utredning av företag får göras, om en säkerhetsutredning förutsätts i en internationell organisations eller ett internationellt organs stadgar eller i en annan stats lag och om utredningen behövs för att den som utredningen gäller ska kunna bli utsedd att delta i ett projekt som ordnas eller annars organiseras av en internationell organisation eller ett internationellt organ eller bli utsedd att delta i ett upphandlingsförfarande som ordnas i en annan stat eller kunna inleda företagsverksamhet i en annan stat (36 § 2 mom.). I de fall som avses i 36 § 2 mom. kan en säkerhetsutredning av företag göras på begäran av företaget i fråga.

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

Vid en säkerhetsutredning av företag ska det med hjälp av uppgifterna i ansökan och de informationskällor som avses i 37 § samt genom inspektion av företagets lokaler och dess informationssystem utredas hur företaget kan se till att information skyddas, obehörigt tillträde till lokalerna förhindras och personalen får utbildning (38 § 1 mom.). Enligt 38 § får en säkerhetsutredning av företag också genomföras partiellt, om det behövs för att uppfylla en internationell förpliktelse som gäller informationssäkerhet eller om det annars är befogat för att syftet med säkerhetsutredningen ska uppnås.

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

Enligt 46 § 2 mom. utfärdar den nationella säkerhetsmyndigheten i enlighet med lagen om internationella förpliktelser som gäller informationssäkerhet sådana intyg över säkerhetsutredning

av företag som behövs för att uppfylla internationella förpliktelser som gäller informationssäkerhet.

2.3 Lagstiftning om behandlingen av personuppgifter

Vid behandlingen av regeringens proposition om godkännande av det administrativa arrangemanget för skydd av säkerhetsklassificerad information som utbyts mellan Finland och Nordatlantiska fördragsorganisationen samt med förslag till lag om sättande i kraft av de bestämmelser som hör till området för lagstiftningen i arrangemanget och i överenskommelsen med Nordatlantiska fördragsorganisationen om informationssäkerhet (RP 139/2012 rd) fäste riksdagens försvarsutskott vid sidan av offentligheten och sekretessfrågorna uppmärksamhet vid kraven på skydd av personuppgifter i propositionen. Utskottet konstaterade utifrån den utredning som utskottet då fick att de bestämmelser som ingår i det administrativa arrangemanget mellan Finland och Nato skapade tillräckliga förutsättningar för att kraven på skydd av personuppgifter ska kunna beaktas vid sidan av offentlighets- och sekretessfrågor. Utskottet underströk att artiklarna i det administrativa arrangemanget bör tolkas och tillämpas med invägande av grundlagens 12 § om offentlighet och 10 § om skydd för personuppgifter när säkerhetsklassificerad information innehåller personuppgifter (FsUB 5/2012 rd).

Enligt 17 § i lagen om internationella förpliktelser som gäller informationssäkerhet har finska myndigheter rätt att till en annan fördragsslutande part lämna ut handlingar och information som är nödvändiga för uppfyllandet av en internationell förpliktelse som gäller informationssäkerhet, trots vad som i finsk lagstiftning föreskrivs om sekretessbeläggning av handlingar och uppgifter. Detta gäller inte uppgifter som är sekretessbelagda på grund av skyddet för privatlivet. I säkerhetsutredningslagens 26 § föreskrivs det om möjligheten att med stöd av ett internationellt avtal inhämta uppgifter ur register som förs av en utländsk myndighet, i 57 § föreskrivs det om myndigheternas rätt att få information och i 59 § om skyldighet att hemlighålla information.

Upprätthållandet av den nationella säkerheten faller med stöd av uttryckliga bestämmelser i akterna i fråga utanför tillämpningsområdet för Europaparlamentets och rådets förordning (EU) 2016/679 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning), nedan *EU:s allmänna dataskyddsförordning* samt Europaparlamentets och rådets direktiv (EU) 2016/680 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF, nedan *dataskyddsdirektivet för brottsbekämpning*. I Finland har dataskyddsdirektivet för brottsbekämpning genomförts genom lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten (1054/2018, nedan *dataskyddslagen avseende brottmål*). Trots begränsningen av tillämpningsområdet för dataskyddsdirektivet för brottsbekämpning har tillämpningsområdet för dataskyddslagen avseende brottmål inom ramen för direktivets handlingsutrymme utvidgats till att gälla behandling av personuppgifter i samband med den nationella säkerheten och försvaret. Således tillämpas i princip dataskyddslagen avseende brottmål på behandlingen av personuppgifter i Natos handlingar när behandlingen omfattas av tillämpningsområdet för 1 § 2 mom. Enligt 1 § 2 mom. i dataskyddslagen avseende brottmål ska den lagen, utöver vad som föreskrivs i 1 mom., tillämpas på

1) sådan behandling av personuppgifter som utförs av Försvarsmakten och för Försvarsmaktens räkning, när uppgifterna behandlas för skötsel av uppgifter som anges i 2 § 1 mom. 1 punkten, 2 punkten underpunkt a eller i 3 eller 4 punkten i lagen om försvarsmakten (551/2007), och på

sådan behandling av personuppgifter som utförs av Försvarsmaktens huvudstab för skötsel av uppgifter som avses i 9 § 3 mom. i säkerhetsutredningslagen,

2) sådan behandling av personuppgifter som utförs av polisen, när uppgifterna behandlas inom ramen för en i 1 kap. 1 § 1 mom. i polislagen (872/2011) avsedd uppgift som hänför sig till skyddet av den nationella säkerheten, och vid uppdrag som avses i 9 § 1 mom. i säkerhetsutredningslagen,

3) sådan behandling av personuppgifter som utförs av Gränsbevakningsväsendet, när uppgifterna behandlas inom ramen för en i 3 § 2 och 3 mom. i gränsbevakningslagen (578/2005) avsedd uppgift som hänför sig till skyddet av den nationella säkerheten.

I 7 kap. i dataskyddslagen avseende brottmål föreskrivs det om den behöriga myndighetens överföring av personuppgifter till tredjeländer och internationella organisationer. I 2 § 1 mom. i lagen om behandling av personuppgifter inom Försvarsmakten (332/2019) har Försvarsmaktens informationsutbyte uteslutits från tillämpningsområdet för 7 kap. i dataskyddslagen avseende brottmål. Bestämmelser om Försvarsmaktens utlämnande av personuppgifter till utlandet och internationella organisationer finns i 4 kap. i lagen om behandling av personuppgifter inom Försvarsmakten.

På behandlingen av personuppgifter i Natos handlingar kan dessutom tillämpas bestämmelser som kompletterar dataskyddslagen avseende brottmål, såsom lagen om behandling av personuppgifter i polisens verksamhet (616/2019) och lagen om behandling av personuppgifter inom Försvarsmakten.

Personuppgifter i Natos handlingar kan också behandlas av andra behöriga myndigheter än de som avses i dataskyddslagen avseende brottmål. På dessa myndigheters behandling av personuppgifter tillämpas i enlighet med 2 § 1 mom. i dataskyddslagen (1050/2018) EU:s allmänna dataskyddsförordning och den nationella dataskyddslagen.

2.4 Riksdagens rätt att få information

Riksdagens rätt att få information och delta i Natoärenden tryggas med stöd av grundlagen och annan lagstiftning. Konstitutionen grundar sig på den i grundlagen föreskrivna principen för demokrati (2 § 1 mom.), enligt vilken riksdagen är det högsta statliga organet också i internationella frågor. Riksdagens ställning som det högsta statliga organet får i detta hänseende konkret innehåll genom det förfarande som tillämpas när skillnaden i synsätt mellan presidenten och statsrådet avgörs (58 § 2 mom.). Riksdagens påverkningsmöjligheter ska också tryggas på ett förutseende sätt.

Statsrådet har det övergripande ansvaret för att riksdagen får information och för att trygga att riksdagen har möjlighet att delta. Enligt principen för parlamentariskt styrelseskick och bestämmelserna i 58 och 93 § i grundlagen har statsrådet också det övergripande ansvaret för beredningen av ärenden.

Riksdagen har enligt 47 § i grundlagen rätt att av statsrådet få de upplysningar som behövs för behandlingen av ett ärende. Bestämmelsen omfattar både statsrådets skyldighet att på eget initiativ tillställa riksdagen behövlig information och skyldigheten att lägga fram sådan information som riksdagen ber om (RP 1/1998 rd, s. 98). Den minister som saken gäller ska se till att utskott eller andra riksdagsorgan utan dröjsmål får handlingar och andra upplysningar som de behöver och som finns hos myndigheterna. Utrikesutskottet ska med stöd av 97 § i grundlagen få utredningar av statsrådet om frågor som gäller utrikes- och säkerhetspolitiken. Utifrån de

utredningar som utrikesutskottet har fått kan det vid behov på eget initiativ ge ett yttrande till statsrådet. Enligt grundlagsutskottet ligger även skyldigheten att redogöra för presidentens utrikespolitiska agerande på statsrådet, som ska ha riksdagens förtroende (GrUB 9/2010 rd). Riksdagen har understrukit att statsrådet självmant ska hålla utrikesutskottet rättidigt och regelbundet underrättat om internationella frågor. Riksdagens roll som skiljedomare i eventuella konflikter kräver information över hela linjen redan när frågor bereds och diskuteras (GrUB 9/2010 rd och UtUU 5/2010 rd).

Enligt grundlagsutskottets tolkning påverkas rätten att få information inte av att de upplysningar ett utskott behöver är sådana till sin juridiska karaktär att de borde hållas hemliga (GrUB 30/2020 rd, s. 3). Även riksdagens utrikesutskott har betonat att riksdagens rätt att få information också gäller sekretessbelagda handlingar (UtUU 4/2020 rd, s. 2). Riksdagens revisionsutskott har konstaterat att de kriterier som ett ministerium skulle kunna tillämpa för att inte behöva lämna riksdagen vissa upplysningar är sannolikt mycket få till antalet och gäller främst fall där upplysningarna är uppenbart oväsentliga och otillförlitliga, spekulativa eller föråldrade. I vissa situationer kan handlingar som berör internationellt samarbete innehålla sådan information vars avslöjande kan medföra betydande och omfattande skada på viktiga allmänna intressen, såsom Finlands relationer med främmande makt. Sådant material ska hanteras på behörigt sätt, vilket man bör fästa särskild vikt vid eftersom det är fråga om Finlands tillförlitlighet som internationell samarbetspartner. Också i fråga om sådan information är det primära tillvägagångssättet med avseende på grundlagen att utskottsmedlemmarna förväntas iaktta sekretess och inte att riksdagen över huvud taget inte får denna information. Grundlagen känner inte till den möjligheten att exempelvis säkerhetsklassificerad information inte lämnas till riksdagen (ReUB 2/2013 rd, s. 3).

Bestämmelser om utskottsmedlemmarnas tystnadsplikt finns i 50 § 2 och 3 mom. i grundlagen och i 43 a–43 c § i riksdagens arbetsordning (GrUU 30/2020 rd, s. 3). Enligt 43 c § 1 mom. i arbetsordningen får en medlem, ersättare eller tjänsteman i ett utskott inte röja en handlings sekretessbelagda innehåll eller en uppgift som vore sekretessbelagd om den ingick i en handling eller en omständighet om vilken utskottet har fattat sekretessbeslut enligt 50 § 3 mom. i grundlagen. Sekretess innebär alltså också att en medlem i det utskott som behandlar ett ärende som omfattas av sekretess inte fritt kan diskutera ärendet exempelvis vid ett gruppmöte (GrUU 30/2020 rd, s. 18). Grundlagsutskottet har understrukit att omfånget för sekretessen bör begränsas till vad som är absolut nödvändigt i fråga om omfattning och varaktighet (GrUU 16/2020 rd s. 5–6). En utskottsmedlem eller en tjänsteman får inte heller använda sekretessbelagda uppgifter för att skaffa sig själv eller någon annan fördel eller för att skada någon annan. Bestämmelser om straff för sekretessbrott och sekretessförseelse finns i 38 kap. 1 och 2 § i strafflagen.

Bestämmelserna om behandling av Natos säkerhetsklassificerade information ska också beaktas vid behandlingen av informationen i riksdagen. Detta innebär till exempel verksamhetsmodeller i enlighet med Natos säkerhetsbestämmelser (inklusive lokal-, person- och informationshanteringslösningar samt tekniska lösningar i anslutning till dem) och utfärdande av intyg över säkerhetsutredning av person i tillämpliga delar. Justitiekanslern i statsrådet har i sin promemoria OKV/3212/24/2021 tagit ställning till riksdagens rätt att få information om särskilt känsligt informationsmaterial i ett ärende som gäller anskaffning av stridsflygplan. I promemorian konstateras det att i internationella förpliktelser som gäller informationssäkerhet är en strikt ändamålsbegränsning ofta viktig för de utlämnade uppgifterna, enligt vilken uppgifterna är tillgängliga endast för ett visst uttryckligt ändamål. Användning av uppgifterna för något annat ändamål förutsätter samtycke av den aktör som har lämnat uppgifterna. I avtalen har det dessutom överenskommits om särskilda förfaranden och skyddsåtgärder för att skydda särskilt känsligt

material. I det nuvarande internationella samarbetet fästs stor vikt vid iakttagandet av förpliktelser som gäller informationssäkerhet och tillbörlig respekt för förpliktelserna är en central del av statens möjligheter att bedriva internationellt samarbete och få information av andra stater.

Av riksdagens ställning som högsta statsorgan samt som statsorgan som utövar lagstiftningsmakt och statsfinansiell makt följer att riksdagen måste få tillförlitlig och omfattande information till grund för sitt beslutsfattande. Detta är en nödvändig förutsättning för de grunder för en demokratisk regeringsform som anges i grundlagen. Informationsutbyte mellan riksdagen och regeringen är oundgängliga element för att det parlamentariska systemet ska fungera. Riksdagens omfattande rätt att få information tryggar också den parlamentariska kontrollen av statsrådet (GrUU 30/2020 rd, s. 2–3).

3 Den internationella utvecklingen samt lagstiftningen i utlandet och i EU

I de internationella överenskommelser och arrangemang som gäller behandling av säkerhetsklassificerad information har man i stor utsträckning etablerat förfaranden och regler för behandlingen av internationell klassificerad information. Finland har i nuläget överenskommelser om informationssäkerhet med 20 stater och med de nordiska länderna, medlemsstaterna i Europeiska unionen, Europeiska rymdorganisationen, Organisationen för gemensamt försvarsmaterielsamarbete i Europa OCCAR och Nordatlantiska fördragsorganisationen. Finland deltar även i den inofficiella multinationella arbetsgrupp för industrisäkerhet som Natos medlemsländer inrättat 1985 (Multinational industrial security working group, *MISWG*), som formulerar gemensamma förfaranden och regler för behandling av information vid utbyte av säkerhetsklassificerad information.

Europeiska unionens förfaranden och regler för behandlingen av säkerhetsklassificerad information påminner till stor del om Natos system. När det gäller rådet ingår de i rådets beslut om säkerhetsbestämmelser för skydd av säkerhetsskyddsklassificerade EU-uppgifter (2013/488/EU). I ett tillägg till beslutet finns en jämförelsetabell för medlemsstaternas säkerhetsklasser. Avtalet mellan Europeiska unionens medlemsstater, församlade i rådet, om skydd av säkerhetsskyddsklassificerade uppgifter som utbyts i Europeiska unionens intresse (FördrS 76 och 77/2015) ingicks 2015. Kommissionen lämnade den 22 mars 2022 ett förslag till Europaparlamentets och rådets förordning om informationssäkerhet i unionens institutioner, organ och byråer (COM(2022) 119 final), som nu är under behandling i rådet och Europaparlamentet. Europeiska unionen har 2003 ingått ett avtal med Nato om informationssäkerhet (2003/211/GUSP, EUT L 80, 27.3.2003, s. 36).

Medlemsstaterna i Europeiska unionen är parter i det ovannämnda avtalet mellan Europeiska unionens medlemsstater, församlade i rådet, om skydd av säkerhetsskyddsklassificerade uppgifter som utbyts i Europeiska unionens intresse. Alla nuvarande medlemsstater i Nato är parter i Natos informationssäkerhetsavtal, som Finland nu ska godkänna. De nordiska länderna har dessutom ingått ett generellt säkerhetsskyddsavtal om ömsesidigt skydd och utbyte av säkerhetsskyddsklassificerade uppgifter mellan Danmark, Finland, Island, Norge och Sverige (FördrS 10–12/2013). De länderna om utgör Finlands referensgrupp har således sinsemellan överensstämmande internationella förpliktelser. Av historiska skäl varierar det länderna emellan hur de nationella säkerhetsmyndigheterna är organiserade. Exempelvis är den nationella säkerhetsmyndigheten (NSA) i Sverige, liksom i Finland, placerad vid utrikesdepartementet, medan den i Danmark finns vid underrättelsetjänsten och i Norge är en tvärsektoriell expert- och tillsynsmyndighet som är underställd försvarsdepartementet men rapporterar till justitiedepartementet i fråga om den civila sektorn. I Nederländerna finns två nationella säkerhetsmyndigheter, AIVD och MIVD. AIVD är en del av inrikesministeriet. Den har ansvar för samordningen i egenskap

av allmän underrättelse- och säkerhetstjänst, men båda myndigheterna kallas inofficiellt nationella säkerhetsmyndigheter (NSA).

4 Avtalets målsättning

I ingressen till avtalet mellan parterna i nordatlantiska fördraget om informationssäkerhet konstateras det att effektivt politiskt samråd, samarbete och planering i försvarsfrågor i syfte att uppnå målen för fördraget förutsätter utbyte av säkerhetsklassificerad information mellan parterna. Detta förutsätter bestämmelser om ömsesidigt skyddande och säkrande av säkerhetsklassificerad information. Syftet med avtalet är att skapa en allmän ram för säkerhetskrav och säkerhetsförfaranden.

5 De viktigaste förslagen

I denna proposition föreslås det att riksdagen godkänner avtalet mellan parterna i nordatlantiska fördraget om informationssäkerhet samt säkerhetsbestämmelserna. Propositionen innehåller också ett förslag till en så kallad blankettlag, genom vilken de bestämmelser i avtalet och i säkerhetsbestämmelserna som hör till området för lagstiftningen sätts i kraft. Det föreslås även att riksdagen ger sitt samtycke till att Finland säger upp det administrativa arrangemanget för skydd av säkerhetsklassificerad information som utbyts mellan Finland och Nordatlantiska fördragsorganisationen samt överenskommelsen med Nordatlantiska fördragsorganisationen om informationssäkerhet. I propositionen ingår ett förslag till lag om upphävande av lagen om sättande i kraft av de bestämmelser som hör till området för lagstiftningen i det arrangemanget och i överenskommelsen (945/2012).

6 Propositionens konsekvenser

6.1 Ekonomiska konsekvenser

Anslutningen till Nato medför tilläggskostnader av engångsnatur och bestående fasta kostnader, bland annat när det gäller informationssäkerhetslösningar och lokalsäkerhet. Kostnaderna för den fortsatta utvecklingen av den informationsbehandlingsmiljö med höga säkerhetskrav som möjliggör behandling av information som gäller Nato bedöms för närvarande uppgå till ca 20 miljoner euro under åren 2023–2025. Det handlar om kostnader för personal, utrustning och programvara. Finansiering för den fortsatta utvecklingen av den informationsbehandlingslösning som ställer höga säkerhetskrav har reserverats i budgeten för 2022 och 2023. Dessutom kommer de skyddsåtgärder som krävs i de lokaler där informationen behandlas att föranleda nya kostnader till ett belopp på uppskattningsvis sex miljoner euro, som huvudsakligen utgörs av hyreskostnader. De investeringar som krävs kommer att medföra underhållskostnader på ca tre miljoner euro från och med 2026.

Det slutliga behovet av finansiering för investeringar och underhåll kommer att preciseras i takt med att planeringen framskrider och planerna genomförs. De lokalkostnader som indirekt föranleds av Natomedlemskapet kommer att preciseras i och med en kartläggning som görs 2023. De övriga eventuella ytterligare kostnaderna i anslutning till bland annat informationsförmedling och lokalsäkerhet kommer att klarna under loppet av flera år. I och med Natomedlemskapet kan den ökade informationsbehandling som ställer höga krav på säkerheten påverka kostnaderna för behandlingen av den information som gäller Nato. Avtalet mellan parterna i nordatlantiska fördraget om informationssäkerhet medför ändå inte direkt några ökade kostnader för statens gemensamma informationsbehandlingsmiljö som förutsätter hög säkerhet, eftersom motsvarande krav har ställts redan under partnerskapstiden.

De ytterligare kostnader som föranleds av att den direkta informationsbehandlingen mellan Försvarsmakten och Nato ökar i och med Natomedlemskapet ingår i Försvarsmaktens budget- och ramförslag. Försvarsmaktens merkostnader beror indirekt på de förpliktelser som gäller informationssäkerheten, men huvudsakligen beror de direkt på själva Natomedlemskapet.

De behov av tilläggsanslag inom olika förvaltningsområden som föranleds av medlemskapet kommer att föras fram i den årliga planen för de offentliga finanserna och vid beredningen av budgeten och tilläggsbudgeten, under moment enligt deras användningsändamål.

6.2 Konsekvenser för myndigheterna

Natomedlemskapets viktigaste konsekvenser för den nationella informationssäkerheten uppkommer genom att olika funktioner ska ordnas på den nivå som Natos informationssäkerhetskrav förutsätter. Finland har ingått en överenskommelse med Nato om skydd av säkerhetsklassificerad information och ett kompletterande administrativt arrangemang, och därmed skyddar och behandlar Finland redan för närvarande Natos säkerhetsklassificerade information i enlighet med minimikraven och de grundläggande principerna i Natos säkerhetsbestämmelser. Kraven gäller personalsäkerhet, datamaterialsäkerhet, lokalsäkerhet, säkerhet i kommunikations- och informationssystem samt industrisäkerhet. Det att Finland förbinder sig till Natos informationssäkerhetsavtal medför ingen avsevärd förändring i jämförelse med nuläget. De små skillnader som finns mellan de informationssäkerhetskrav som tillämpats under partnerskapet för fred och de som ska tillämpas under medlemskapet behandlas i avsnitt 8.2. De informationssäkerhetsförfaranden som etablerats under partnerskapet för fred utgör en fungerande grund för det arbete med att utveckla förfarandena som tar vid när Finland blir medlem. I och med medlemskapet ökar mängden säkerhetsklassificerad Natoinformation, och flera olika myndigheter, ministerier och företag kommer att behöva behandla sådan information. Innan Finland blivit medlem är det dock svårt att bedöma i vilken utsträckning antalet handlingar kommer att öka inom de olika förvaltningsområdena. I och med medlemskapet kan Finland också få handlingar i Natos högsta säkerhetsklass (COSMIC TOP SECRET), som i regel inte lämnas ut till aktörer utanför medlemsstaterna.

Natos säkerhetsbyrå gjorde ett kontrollbesök i Finland den 3–6 maj 2022. Under besöket utvärderades skyddet av Natos säkerhetsklassificerade information. Enligt slutledningarna av kontrollen bör myndigheterna utvärdera och till den del det behövs utöka resurserna för skydd av Natos säkerhetsklassificerade information. Detta gäller uttryckligen den nationella säkerhetsmyndigheten och säkerhetsutredning av person, personalen vid registratorskontoren, processen för godkännande av informationssystem och elektroniska behandlingsmiljöer samt lokalsäkerhet och industrisäkerhet. Vid Huvudstaben har man identifierat ett behov av att stärka expertresurserna inom dessa områden. Inom Försvarsmakten ökar behovet av normala och i synnerhet omfattande säkerhetsutredningar av person. Även behovet av sådana säkerhetsutredningar av företag som görs av Huvudstaben kan öka. Detta leder till ett ökat behov av personalresurser vid Huvudstaben.

Medlemskapet i Nato kommer att medföra en ökad mängd säkerhetsklassificerad Natoinformation i Finland. Nato rekommenderar i första hand elektronisk överföring och behandling av säkerhetsklassificerad information för skydd av informationen. Elektronisk informationsöverföring är också ur nationell synvinkel nödvändig för att säkerställa att det operativa samarbetet och beslutsfattandet är rättidigt. När elektroniska informationsbehandlingsmiljöer införs bör behoven hos de olika ministerierna, Finlands beskickningar utomlands, republikens presidents kansli samt ämbetsverken och i synnerhet Försvarsmakten beaktas. Handlingar kommer att distribueras till olika förvaltningsområden, men ökningen kommer att märkas särskilt inom Försvarsmakten och vid utrikesministeriet och försvarsministeriet. Det är nödvändigt att så fort som

möjligt utveckla en sådan nationell miljö för säkerhetsklass II som är godkänd också för behandling av information i säkerhetsklassen NATO SECRET. Genomförandet av den elektroniska behandlingsmiljön stöder sig delvis på beslutet om hur registerfunktionerna ska förverkligas nationellt. Modellerna för genomförandet av en elektronisk informationsbehandlingsmiljö och registerfunktionerna är för närvarande föremål för nationell prövning.

Enligt Natos informationssäkerhetskrav får säkerhetsklassificerad information från och med nivån NATO CONFIDENTIAL behandlas och förvaras endast inom ett säkert utrymme med behörighetskontroll som är fysiskt skyddat och godkänt av en myndighet. Information i säkerhetsklassen NATO RESTRICTED ska behandlas inom ett sådant administrativt område som myndigheten har godkänt. Inrättandet av fysiska behandlingsmiljöer medför avsevärda kostnader inom hela statsförvaltningen.

Enligt Natos säkerhetsbestämmelser ska alla informationssystem där säkerhetsklassificerad Natoinformation behandlas genomgå en process för godkännande. Detta gäller de system som Nato tillhandahåller Finland och de nationella system i Finland där Natos säkerhetsklassificerade information behandlas. När det gäller de system som Nato tillhandahåller är det Transport- och kommunikationsverket som svarar för ackrediteringen av systemets nationella åtkomstpunkt och lämnar utlåtande om ackrediteringen (Statement of Compliance) till Natos nämnd för säkerhetsgodkännande. Processen för godkännande av de nationella informationssystem i vilka Natos säkerhetsklassificerade information behandlas består av riskbedömning, definition av kraven på systemen, kontroller och ackreditering, acceptans av den kvarstående risken utifrån utlåtandet om ackrediteringen samt beviljande av tillstånd att använda systemen. Utlåtandet om ackreditering är i kraft i tre år. Det har bedömts att arbetet med kontroller och godkännande av de system i vilka Natos säkerhetsklassificerade information behandlas kommer att medför ett permanent behov av ytterligare resurser vid Transport- och kommunikationsverket.

Den nationella helheten av informationssystem för behandling av säkerhetsklassificerad Natoinformation måste uppfylla Natos krav på säkerhet för informationssystem. Transport- och kommunikationsverket ger myndigheterna vägledning i planeringen av säkerhetskraven för systemen, vilket stöder en smidig godkännandeprocess. Detta stöd för planeringen av den nationella systemhelheten samt tryggandet av en effektiv bedömningsprocess förutsätter att verket får ytterligare resurser.

Vid behandlingen av regeringens proposition RP 315/2022 rd fäste riksdagens underrättelsetillsynsutskott, med tanke på resurstilldelningen för de åtgärder som krävs för att sörja för informations- och lokalsäkerheten, uppmärksamhet vid att den nationella säkerhetsmyndigheten och de utsedda säkerhetsmyndigheter som avses i lagen om internationella förpliktelser som gäller informationssäkerhet får fler uppgifter (UndUU 1/2022 rd, s. 3).

6.3 Konsekvenser för näringslivet

Informationssäkerhetsavtalet ger finska företag en möjlighet att bli utsedda att delta i projekt som ordnas eller annars organiseras av Nato eller bli utsedda att delta i ett upphandlingsförfarande som ordnas i en annan stat och som förutsätter behandling av säkerhetsklassificerad Natoinformation.

Projekt som inbegriper säkerhetsklassificerad information finns speciellt inom försvarsindustrin, inom säkerhet, kärnkraft, informationsteknik och andra högteknologiska sektorer samt inom vetenskap och forskning. Utan informationssäkerhetsavtalet skulle finska företag inte kunna delta i Natoprojekt som omfattar säkerhetsklassificerad information. Det kan i enlighet

med avtalet krävas ett sådant intyg över säkerhetsutredning av företag som avses i 46 § i säkerhetsutredningslagen för att ett företag ska bli utsett att delta i ett projekt. För säkerhetsutredningar av företag tas det i enlighet med säkerhetsutredningslagen hos företaget ut en avgift med iakttagande av lagen om grunderna för avgifter till staten (150/1992).

Avtalet syftar till att göra det möjligt för finska företag att delta i projekt och därmed öka deras konkurrenskraft och utrikeshandel.

7 Remissvar

Utkastet till proposition var på remiss mellan den 24 mars och 21 april 2023. Utlåtande begärdes av xx remissinstanser. Sammanlagt lämnades xx utlåtanden. Begäran om utlåtande och utlåtandena finns tillgängliga på adressen valtioneuvosto.fi/sv/projekt under projektnumret UM001:00/2023.

8 Bestämmelserna i avtalet mellan parterna i nordatlantiska fördraget om informationssäkerhet och deras förhållande till lagstiftningen i Finland

8.1 Avtalet mellan parterna i nordatlantiska fördraget om informationssäkerhet

Inledning. I avtalsingressen bekräftas att effektivt politiskt samråd, samarbete och planering i försvarsfrågor i syfte att uppnå målen för det nordatlantiska fördraget förutsätter utbyte av säkerhetsklassificerad information mellan parterna. I ingressen konstateras det även att utbytet av information förutsätter sådana bestämmelser om ömsesidigt skyddande och säkrande av säkerhetsklassificerad information som tillämpas mellan parterna i nordatlantiska fördraget. För sådana säkerhetskrav och säkerhetsförfaranden behövs det en allmän ram, om vilken det överenskoms i avtalet.

Artikel 1. Enligt artikel 1 punkt i förbinder sig parterna att skydda och säkra säkerhetsklassificerad information som definieras närmare i bilaga I till avtalet och som härrör från Nato eller som en medlemsstat lämnar till Nato samt medlemsstaternas säkerhetsklassificerade information som är märkt som sådan och som lämnas till en annan medlemsstat som stöd för Natos program, projekt eller kontrakt.

Avtalet lämpar sig således inte bara för säkerhetsklassificerad information som utbyts mellan Finland och Nato utan också för säkerhetsklassificerad information som utbyts mellan medlemsstaterna och som lämnas som stöd för Natos program, projekt eller kontrakt. Tillämpningen av avtalet mellan medlemsstaterna förutsätter således inget formellt samarbete inom Nato, utan det tillämpas också på sådant internationellt samarbete mellan medlemsstaterna som stöder Natos verksamhet. Enligt artikel 3 i det nordatlantiska fördraget ska parterna, var för sig och tillsammans, genom kontinuerlig och effektiv egen beredskap och ömsesidigt bistånd, upprätthålla och utveckla sin individuella och kollektiva förmåga att stå emot väpnade angrepp. I artikeln avsett samarbete kan genomföras mellan medlemsstaterna utan att det sker inom ramen för Natos formella samarbetsformer och utan att Natos organ deltar. Natos informationssäkerhetsavtal tillämpas också på medlemsstaternas nationellt säkerhetsklassificerade information som utbyts vid sådant bilateralt eller multilateralt samarbete. Ofta hänvisas det också i internationella avtalshandlingar som definierar sådant samarbete till Natos krav på informationssäkerhet eller nivån på skyddet av dem. Avtalet kan dessutom främja utbytet av nationell säkerhetsklassificerad information mellan Natos medlemsstater också i andra situationer, om det inte finns något bilateralt fördrag om informationssäkerhet och om båda parterna anser att det är lämpligt.

Enligt artikel 1 punkt ii ska parterna bevara säkerhetsklassificeringen av den information som avses i punkt i och göra sitt yttersta för att säkra informationen i enlighet därmed. Enligt artikel 1 punkt iii ska den säkerhetsklassificerade information som anges i punkt i inte användas för andra ändamål än de som anges i nordatlantiska fördraget och i beslut och resolutioner som hänför sig till fördraget. Bestämmelsen innehåller den finalitetsprincip som vanligen ingår i internationella överenskommelser om informationssäkerhet. Enligt artikel 1 punkt iv ska parterna inte utan samtycke av den från vilken informationen härrör avslöja informationen för sådana parter som inte hör till Nato.

På avtalet tillämpas efter det att avtalet har satts i kraft lagen om internationella förpliktelser som gäller informationssäkerhet. Bestämmelserna om åtgärder som gäller informationssäkerhet i 3 kap. i den lagen innehåller de bestämmelser som behövs för genomförandet av bestämmelserna i artikel 1.

Artikel 2. Enligt artikel 2 ska parterna säkerställa att en nationell säkerhetsmyndighet, som ska vidta skyddande säkerhetsåtgärder, inrättas för Natos verksamhet. Parterna ska utarbeta och tillämpa säkerhetskrav, som ska säkerställa en gemensam skyddsnivå för säkerhetsklassificerad information. Dessa säkerhetskrav beskrivs närmare i avsnitt 8.2 nedan.

Bestämmelser om de krav som ställs på behandlingen av säkerhetsklassificerad information finns i lagen om internationella förpliktelser som gäller informationssäkerhet, lagen om informationshantering inom den offentliga förvaltningen och säkerhetsklassificeringsförordningen. Säkerhetsklassificeringsförordningen tillämpas på behandlingen av Natos säkerhetsklassificerade handlingar, om inte något annat följer av en internationell förpliktelse som gäller informationssäkerhet.

Bestämmelserna i 3 kap. i lagen om internationella förpliktelser som gäller informationssäkerhet innehåller de på lagnivå viktigaste åtgärderna som gäller informationssäkerhet: sekretess och användning av information (6 §), tystnadsplikt och förbud mot utnyttjande (7 §), anteckning om säkerhetsklass (8 §), mot säkerhetsklassen svarande hanteringskrav (9 §) och säkerhetskrav som gäller utrymmen (10 §).

I 6–15 § i säkerhetsklassificeringsförordningen föreskrivs det om informationssäkerhetsåtgärder som ska vidtas vid behandlingen av säkerhetsklassificerade handlingar och som i enlighet med internationella förpliktelser som gäller informationssäkerhet och handlingens livscykel hänför sig till förutsättningarna för utlämnande av en handling (6 §), skydd på flera nivåer (7 §), beviljande av behandlingsrättigheter och förteckningen över dem (8 §), säkerhetsområden, dvs. lokalsäkerhet (9 §), skydd av behandlingen av handlingar och av informationssystemen med hjälp av säkerhetsområden (10 §), krav som gäller informationssystem och datakommunikationsarrangemang (11 §), överföring av en handling via datanätet (12 §), transport av en handling (13 §), uppföljning av behandlingen av en handling (14 §) och förstöring av handling (15 §).

Enligt 4 § i lagen om internationella förpliktelser som gäller informationssäkerhet är utrikesministeriet Finlands nationella säkerhetsmyndighet vid uppfyllandet av internationella förpliktelser som gäller informationssäkerhet. Försvarsministeriet, Huvudstaben, Skyddspolisen och Transport- och kommunikationsverket är utsedda säkerhetsmyndigheter. Den nationella säkerhetsmyndigheten har till uppgift att i synnerhet styra och övervaka att det särskilt känsliga informationsmaterial som avses i lagen skyddas och att det hanteras på ett lämpligt sätt.

De utsedda säkerhetsmyndigheterna utför de uppgifter som föreskrivs för dem i lagen om internationella förpliktelser som gäller informationssäkerhet och andra uppgifter som följer av internationella förpliktelser som gäller informationssäkerhet. Försvarsministeriet, Huvudstaben och Skyddspolisen är den nationella säkerhetsmyndighetens sakkunniga i ärenden som gäller personalsäkerhet, företagssäkerhet och lokalsäkerhet samt Transport- och kommunikationsverket i ärenden som gäller informationssäkerhet i fråga om informationssystem och datakommunikation.

Den nationella säkerhetsmyndigheten har offentliggjort verktyget Katakri, i vilket de minimikrav som grundar sig på nationella författningar och internationella förpliktelser har sammanställts. Katakri är myndigheternas verktyg för auditering av informationssäkerhet som kan användas för att bedöma den berörda organisationens förmåga att skydda nationellt eller internationellt säkerhetsklassificerad information. Katakri ställer inte i sig några absoluta krav på informationssäkerheten, utan de insamlade kraven grundar sig på gällande lagstiftning och på de internationella förpliktelser som gäller informationssäkerhet och som är bindande för Finland. Kraven har beskrivits så att de möjliggör olika genomförandesätt. I fälten för tilläggsuppgifter har man till stöd för tolkningen samlat exempel på olika genomförandesätt. Genom de i exemplen beskrivna förfarandena kan man i de flesta miljöer uppnå en godtagbar miniminivå för skyddet. Exemplen på olika genomförandesätt är inte bindande och de kan också ersättas med skyddsåtgärder på motsvarande nivå.

Den nationella säkerhetsmyndigheten har för avsikt att i samarbete med de utsedda säkerhetsmyndigheterna publicera en Nato-bilaga som kompletterar Katakri i syfte att stödja de organisationer inom den offentliga förvaltningen och näringslivet som kommer att behandla Natos säkerhetsklassificerade information. Bilagan baserar sig på Natos preciserande säkerhetsbestämmelser och säkerhetsdirektiv som överlämnades till Finland 2022 och av vilka man har gjort en jämförande analys i Katakri. Bilagan medför inga betydande ändringar av innehållet i eller tillämpningen av Katakri, utan bilagans syfte är enbart att visa på beaktansvärda skillnader mellan de nationella säkerhetskraven och Natos säkerhetskrav.

Vid indelningen i säkerhetsområden enligt den gällande säkerhetsklassificeringsförordningen och i reglerna för behandling av handlingar (9 och 10 §) har beaktats Europeiska unionens råds säkerhetsbestämmelser, enligt vilka säkerhetsklassificerad information som hör till säkerhetsklass CONFIDENTIAL (säkerhetsklass III) eller SECRET (säkerhetsklass II) får behandlas inom ett administrativt utrymme, om åtkomsten till uppgifterna skyddas från utomstående. Natos säkerhetsstrategi möjliggör dock behandling av information högst i säkerhetsklass NATO RESTRICTED (säkerhetsklass IV) inom administrativa utrymmen. Denna skillnad i behandlingsreglerna och behövliga jämförelser anges i Nato-bilagan till Katakri. Säkerhetsklassificeringsförordningen tillämpas i Finland på behandlingen av såväl nationell som internationell säkerhetsklassificerad information, om inte något annat följer av en internationell förpliktelse som gäller informationssäkerhet. De miniminormer som beskrivs i Natos säkerhetsstrategi utgör en sådan internationell förpliktelse som är bindande för Finland och vars bestämmelser blir tilllämpliga vid behandlingen av information som härrör från Nato.

Artikel 3. Enligt artikel 3.1 förbinder sig parterna att säkerställa att alla deras medborgare som i sina arbetsuppgifter behöver eller kan komma att få tillgång till information i säkerhetsklass CONFIDENTIAL eller högre genomgår en relevant säkerhetsutredning innan de åtar sig sitt uppdrag. I Natos säkerhetsbestämmelser förs det fram att exempelvis stats- och regeringschefers, statsrådets ministrars, riksdagsledamöters och domstolsväsendets medlemmars tillgång till information ändå grundar sig på nationell lagstiftning. Även dessa personer ska informeras om sina säkerhetsförpliktelser och ha behovsenlig behörighet till informationen (need to know).

Artikel 3.2 innehåller ett krav på förfarandena för säkerhetsutredningar. Med hjälp av dem ska det fastställas huruvida personen i fråga, med beaktande av hur lojal och pålitlig personen är, kan ges tillgång till säkerhetsklassificerad information utan att detta medför en oacceptabel säkerhetsrisk.

Artikel 3.3 förutsätter att parterna på begäran samarbetar med de andra parterna i samband med genomförandet av deras säkerhetsutredningsförfaranden.

Enligt 11 § i lagen om internationella förpliktelser som gäller informationssäkerhet ska en sådan säkerhetsutredning av person som förutsätts i en internationell förpliktelse som gäller informationssäkerhet göras på det sätt som föreskrivs i säkerhetsutredningslagen. Ett intyg över säkerhetsutredning av person utfärdas dock av den nationella säkerhetsmyndigheten, om inte något annat följer av särskilda skäl. I 26 § i säkerhetsutredningslagen föreskrivs det om inhämtande av uppgifter ur register som förs av utländska myndigheter. I 17 § i lagen om internationella förpliktelser som gäller informationssäkerhet föreskrivs det om utlämnande av handlingar och information som behövs för uppfyllande av en internationell förpliktelse som gäller informationssäkerhet till en part i en internationell överenskommelse om informationssäkerhet.

Artikel 4. Enligt artikeln ska Natos generalsekreterare säkerställa att Nato tillämpar de i respektive fall tillämpliga bestämmelserna om skydd av säkerhetsklassificerad information i avtalet. En precisering av detta finns i bilaga III till avtalet.

Nato har antagit sådana detaljerade bestämmelser som avses i denna artikel och som tillämpas både på medlemsstaternas och på Natos verksamhet. Inom Nato är det Natos säkerhetsbyrå (Nato Office of Security, NOS) som samordnar, övervakar och verkställer Natos säkerhetsstrategi (Nato Security Policy).

Artikel 5. Enligt artikeln hindrar avtalet inte på något sätt att parterna ingår andra avtal som inte påverkar tillämpningsområdet för avtalet och som gäller utbyte av sådan säkerhetsklassificerad information som härrör från parterna.

Finland har i nuläget bilaterala överenskommelser om informationssäkerhet med 20 stater och med de nordiska länderna, medlemsstaterna i Europeiska unionen, Europeiska rymdorganisationen, Organisationen för gemensamt försvarsmaterielsamarbete i Europa OCCAR och Nordatlantiska fördragsorganisationen. Den tidigare överenskommelsen med Nato liksom det administrativa arrangemanget ersätts med det avtal som nu föreslås bli godkänt.

Artikel 6. Avtalet har varit öppet för undertecknande av de dåvarande medlemsstaterna i Nato, vilkas ratifikations-, godtagande- eller godkännandeinstrument skulle deponeras hos Amerikas förenta staters regering. Enligt artikel 6 punkt b har avtalet trätt i kraft 30 dagar efter den dag då två signatärstater har deponerat sina ratifikations-, godtagande- eller godkännandeinstrument. Avtalet trädde enligt bestämmelsen i kraft internationellt den 16 augusti 1998. Efter detta har avtalet i fråga om alla andra signatärstater trätt i kraft 30 dagar efter det att respektive stats ratifikations-, godtagande- eller godkännandeinstrument har deponerats.

Enligt artikel 6 punkt c har avtalet ersatt den handling som Nordatlantiska rådet i bilaga A (punkt 1) till tillägget till bilagan till handling D.C.2/7 godkände den 19 april 1952 och som senare inkluderats i bilaga A till handling C-M(55)15(Final), som godkändes av Nordatlantiska rådet den 2 mars 1955.

Artikel 7. Artikeln innehåller en för Finland tillämplig bestämmelse om anslutning till informationssäkerhetsavtalet. Avtalet ska vara öppet för anslutning av en ny part i nordatlantiska fördraget i enlighet med dennes konstitutionella förfaranden. Anslutningsinstrumentet ska deponeras hos Amerikas förenta staters regering. Avtalet ska träda i kraft för varje anslutande stat 30 dagar efter den dag då dess anslutningsinstrument deponerades. Finland har vid anslutningsförhandlingarna förbundit sig att ansluta sig till informationssäkerhetsavtalet inom 12 månader från deponeringen av Finlands anslutningsinstrument för nordatlantiska fördraget.

Artikel 8. Amerikas förenta staters regering ska underrätta regeringarna för de andra parterna om deponeringen av varje ratifikations-, godtagande-, godkännande- eller anslutningsinstrument.

Artikel 9. Artikeln innehåller bestämmelser om uppsägning av avtalet. Avtalet kan sägas upp av varje part genom skriftligt meddelande om uppsägning till depositarien, som ska underrätta samtliga andra parter om varje sådant meddelande. Uppsägningen börjar gälla ett år från det att meddelandet mottagits av depositarien, men den ska inte påverka de förpliktelser, rättigheter eller maktbefogenheter som parterna tidigare har kommit överens om eller fått på grundval av bestämmelserna i avtalet.

Giltiga texter. Avtalets autentiska språk är engelska och franska. Depositarie för avtalet är Amerikas förenta staters regering.

Bilaga I. Bilagorna till avtalet utgör en integrerad del av avtalet. I bilaga I definieras Natos säkerhetsklassificerade information. Enligt punkt a i bilagan avser ”information” sådan information som kan förmedlas i vilken form som helst. Enligt punkt b i bilagan avser ”säkerhetsklassificerad information” information eller material som anses kräva skydd mot obehörigt röjande och som med säkerhetsklassificering har angetts vara sådan. Enligt punkt c i bilagan omfattar ”material” handlingar och även maskiner, utrustning och vapen som tillverkats eller är under tillverkning. Enligt punkt d i bilagan avser ”handling” all lagrad information oberoende av dess fysiska form eller egenskaper, inklusive utan inskränkningar skriftliga dokument och trycksaker, kort och band som används vid databehandling, kartor, diagram, fotografier, målningar, ritningar, gravyrer, utkast, arbetsanteckningar och arbetspapper, kolpapperkopior och färgband, kopior oberoende av på vilket sätt eller med vilken metod de gjorts, alla slags ljud-, tal- och magnetupptagningar samt elektroniska och optiska upptagningar och videoupptagningar, bärbara adb-apparater med fasta lagringsmedier och löstagbara lagringsmedier för datorer. I den nationella lagstiftningen definieras myndighetshandling i 5 § i offentlighetslagen.

Bilaga II. I bilagan definieras vad som i avtalet avses med Nato. Med ”Nato” avses Nordatlantiska fördragsorganisationen och de organ på vilka antingen avtalet om status för Nordatlantiska fördragsorganisationen, nationella representanter och organisationens internationella personal, undertecknat i Ottawa den 20 september 1951, eller protokollet om status för de internationella militära högkvarter som inrättats enligt Nordatlantiska fördraget, undertecknat i Paris den 28 augusti 1952, tillämpas.

Bilaga III. Bilagan innehåller en bestämmelse som kompletterar artikel 4 i avtalet och enligt vilken samråd ska föras med militära befälhavare för att respektera deras maktbefogenheter. Militärkommittén ansvarar för alla säkerhetsfrågor inom Natos militära struktur och cheferna för Natos militära organ som inrättats under kommittén ansvarar för alla säkerhetsfrågor inom sina respektive organisationer. Enligt säkerhetsbestämmelserna ska säkerhetsbyrån till exempel informera ordföranden för militärkommittén om Natos säkerhetssituation samt om hur genomförandet av NAC:s säkerhetsbeslut framskrider.

8.2 Natos krav och delområden inom informationssäkerhet

Natos säkerhetsverksamhet baserar sig på Natos internt godkända säkerhetsstrategi (Nato Security Policy) och på medlemsstaternas säkerhetsförfaranden som bygger på den. I fråga om Nato har de grundläggande principerna och miniminormerna för den gemensamma skyddsnivå som avses i artikel 2 i informationssäkerhetsavtalet fastställts i Natos handling C-M(2002)49-REV1, ”Security within the North Atlantic Treaty Organization” (nedan Natos säkerhetsbestämmelser), de direktiv som stöder den (*directives*), riktlinjer (*guidelines*) och tolkningsanvisningar (*supporting documents*). Enligt säkerhetsbestämmelserna ska medlemsstaterna se till att de tillämpar de grundläggande principer och miniminormer som anges i säkerhetsbestämmelserna så att Natos säkerhetsklassificerade information skyddas mot förlust av konfidentialitet, fullständighet och tillgänglighet.

Säkerhetsstrategin ställer upp grundläggande principer och miniminormer för säkerhet så att Natos säkerhetsklassificerade information ska få ett verifierat skydd som överensstämmer med kraven i medlemsländerna och i Natos organ. Säkerhetsstrategin bildar en omfattande och detaljerad helhet som gäller genomförandet av informationssäkerhetsavtalet, men utgör dock inte en del av avtalet.

Parterna utvärderar och uppdaterar Natos säkerhetsstrategi i olika sammansättningar. Frågor som gäller Natos informationssäkerhet behandlas i Natos säkerhetskommittés säkerhetspolitiska sammansättning. Sekretariatet för kommittén är Natos säkerhetsbyrå (NOS (*NATO Office of Security*)), som också tillsätter kommitténs ordförande. Kommitténs medlemmar består av medlemsstaternas nationella (NSA, National Security Authority) och/eller utsedda säkerhetsmyndigheter (DSA, Designated Security Authority). Finland har deltagit i kommitténs arbete sedan 2011. Säkerhetskommittén har också en CISS-sammansättning för teknisk informationssäkerhet (NATO SC (CISS)). Natos civila och militära organ ansvarar för säkerhetsfrågor inom sina ansvarsområden.

Delområdena för informationssäkerhet i Natos säkerhetsstrategi är personalsäkerhet, fysisk säkerhet, datamaterialsäkerhet, säkerhet i kommunikations- och informationssystem samt industrisäkerhet. Åtgärderna omfattar personer, system, lokaler, infrastruktur och miljö samt kontroll av behandlingen av information och informationshantering. De centrala säkerhetskraven för dessa ingår i bilagorna B–H till Natos säkerhetsregler C-M(2002)49-REV1. Innehållet i dessa bilagor beskrivs nedan.

Bilaga A - Avtalet mellan parterna i nordatlantiska fördraget om informationssäkerhet

Bilaga A till säkerhetsbestämmelserna innehåller texten till det egentliga informationssäkerhetsavtalet, vars innehåll det redogörs för ovan i avsnitt 8.1.

Bilaga B – Grundläggande principer, miniminormer och ansvar

I bilaga B till säkerhetsbestämmelserna beskrivs de grundläggande principerna, miniminormerna och ansvaren i anslutning till tillämpningen av Natos säkerhetsbestämmelser, genom tillämpningen av vilka Natos medlemsstater och Natos militära och civila organ säkerställer en gemensam skyddsnivå för säkerhetsklassificerad information som utbyts mellan parterna.

De grundläggande principer och miniminormer som beskrivs hänför sig bland annat till begränsning av rätten att behandla säkerhetsklassificerad information, beaktande av interna hot som en del av säkerhetsförfarandena, ordnande av utbildning i säkerhet, skyldigheten att rapportera säkerhetsöverträdelser och förfarandet för rapportering samt upphovsmannens kontroll över sådan

säkerhetsklassificerad information som denne lämnat ut. Utlämnandet av Natos säkerhetsklassificerade information ska ske i enlighet med de fastställda förfarandena och kriterierna för utlämnande och informationen ska skyddas av en nivå som är minst lika strikt som den som anges i Natos säkerhetsbestämmelser och de stödjande direktiven.

Miniminormerna för Natos säkerhetsklassificerade information ska utsträckas till att omfatta alla personer som har tillgång till säkerhetsklassificerad information samt alla lokaler och utrymmen och medier där sådan information hanteras. Sådan information får endast spridas utifrån behovsenlig behörighet som hänför sig till en officiell uppgift. I fråga om informationsmaterial i säkerhetsklass NATO CONFIDENTIAL och högre förutsätts det dessutom att de personer som hanterar informationen har genomgått en relevant säkerhetsutredning och har instruerats om de säkerhetsförfaranden som tillämpas vid hanteringen. Förutsättningarna för hantering av säkerhetsklassificerad information ska bedömas också efter det att ett intyg över säkerhetsutredning har utfärdats genom olika uppföljningsåtgärder som syftar till att göra det möjligt att hantera interna hot som hänför sig risken att information läcker.

Den nationella säkerhetsmyndigheten i en medlemsstat i Nato ansvarar för säkerheten för Natos säkerhetsklassificerade information och är den främsta kontaktpunkten för Natos säkerhetsbyrå när det gäller alla säkerhetsfrågor i Nato. Vid behov kan myndigheten hänvisa Natos säkerhetsbyrå till någon annan behörig säkerhetsmyndighet. Den nationella säkerhetsmyndigheten ansvarar för säkerheten för Natos säkerhetsklassificerade information i såväl militära som civila nationella byråer och enheter i hemlandet och utomlands. Den ansvarar för att säkerställa att regelbundna och lämpliga inspektioner utförs i alla nationella organisationer för att fastställa att Natos säkerhetsklassificerade information skyddas på lämpligt sätt och att personer som hanterar säkerhetsklassificerad information har beviljats ett intyg över personalsäkerhetsgodkännande i enlighet med Natos säkerhetsstrategi. Den nationella säkerhetsmyndigheten ska också godkänna att nationella Cosmiccentralregister inrättas och avvecklas. De utsedda säkerhetsmyndigheterna ansvarar för att informera industrin om den nationella strategin i alla frågor som gäller Natos industrisäkerhetsstrategi och för att ge bistånd vid dess genomförande.

Ett säkerhetsärende i Nato som inte kan lösas eller ett ärende som gäller genomförande eller tolkning av Natos säkerhetsstrategi mellan Natos medlemsstaters nationella säkerhetsmyndigheter eller utsedda säkerhetsmyndigheter och Natos militära eller civila organ ska föras till Natos säkerhetsbyrå för avgörande. Natos säkerhetsbyrå hänskjuter olösta meningsskiljaktigheter till Natos säkerhetskommitté.

Förslag från Natos medlemsstater och Natos militära och civila organ om ändring av Natos säkerhetsstrategi ska i första hand lämnas till Natos säkerhetsbyrå för behandling. Natos säkerhetsbyrå ska behandla förslagen och vid behov hänskjuta dem till Natos säkerhetskommitté för fortsatt behandling. Medlemsstaternas nationella säkerhetsmyndigheter och utsedda säkerhetsmyndigheter får trots detta lägga fram formella förslag till ändring av säkerhetsstrategin för Natos säkerhetskommitté, om de så önskar.

Bilaga C – Personalsäkerhet

I bilaga C till säkerhetsbestämmelserna beskrivs strategin och miniminormerna för personalsäkerhet i säkerhetsbestämmelserna. De allmänna principer som beskrivs i bilagan stöds av Natos mer detaljerade direktiv om personalsäkerhet AC/35-D/2000. Kraven på personalsäkerhet definierar under vilka förutsättningar personer kan ges tillgång till Natos säkerhetsklassificerade information.

Medlemsstaternas förfaranden för personalsäkerhet ska vara tillräckliga för att fastställa om en person med beaktande av vederbörandes lojalitet, tillförlitlighet och pålitlighet kan beviljas tillgång till Natos säkerhetsklassificerade information utan att den säkerhetsrisk som detta medför överstiger en acceptabel nivå. Alla civila och militära personer vars arbetsuppgifter förutsätter tillgång till uppgifter i säkerhetsklass CONFIDENTIAL eller högre ska genomgå en relevant säkerhetsutredning och ha ett intyg över personalsäkerhetsgodkännande (PSC), om tillräcklig förtroendenivå har uppnåtts i fråga om deras lämplighet att få tillgång till sådan information. Ett undantag från PSC-kravet utgörs av innehavarna av statens högsta ämbeten (stats- och regeringschefer, ministrar, riksdagsledamöter och medlemmar av rättsväsendet), i fråga om vilka tillgången till Natos säkerhetsklassificerade information grundar sig på nationella lagar och andra författningar. De sistnämnda personerna ska dock informeras om de säkerhetsförpliktelser som hänför sig till behandlingen av uppgifter och de ska ha behovsenlig behörighet för behandlingen av uppgifterna.

Personer från Natos medlemsstater samt Natos civila och militära organ har tillgång endast till sådan säkerhetsklassificerad information som de har behovsenlig behörighet till (need-to-know). Ingen har rätt att få tillgång till Natos säkerhetsklassificerade information enbart på basis av personens ställning, tjänst eller intyg över personalsäkerhetsgodkännande.

Det ska säkerställas att lämplig säkerhetsutbildning ordnas för alla personer som har tillgång till Natos säkerhetsklassificerade information eller som har ett personalsäkerhetsgodkännande för behandling av säkerhetsklassificerad information. Personer som behandlar sådan information ska informeras om de säkerhetsförfaranden som hänför sig till behandlingen av informationen och om deras säkerhetsförpliktelser samt regelbundet påminnas också om de olika säkerhetshot som är förenade med behandlingen av informationen. Alla personer som har genomgått en säkerhetsutredning ska bekräfta att de fullt ut förstår sitt ansvar och de eventuella följderna för dem, om Natos säkerhetsklassificerade information hamnar i obehöriga händer, antingen uppsåtligen eller av oaktsamhet.

Det detaljerade ansvaret för nationella säkerhetsmyndigheter och utsedda säkerhetsmyndigheter eller andra behöriga säkerhetsmyndigheter, Natos medlemsstater och Natos chefer för civila eller militära organ anges i direktivet om personalsäkerhet (AC/35-D/2000).

Bilaga D – Fysisk säkerhet

I bilaga D till säkerhetsbestämmelserna beskrivs strategin och miniminormerna för fysisk säkerhet till skydd för Natos säkerhetsklassificerade information. Närmare information om de detaljerade kraven på fysisk säkerhet finns i Natos direktiv om fysisk säkerhet (AC/35-D/2001), som stöder Natos säkerhetsstrategi.

Natos medlemsstater ska upprätta fysiska säkerhetsprogram, som omfattar aktiva och passiva säkerhetsåtgärder och som skapar en gemensam nivå av fysisk säkerhet som motsvarar bedömningen av hot mot, sårbarheter hos samt säkerhetsklassificering och mängd av den information som ska skyddas. Alla platser, byggnader, verksamhetsställen och andra utrymmen där Natos säkerhetsklassificerade information hanteras eller diskuteras ska skyddas genom lämpliga fysiska säkerhetsåtgärder. Syftet med dessa säkerhetsåtgärder är att förhindra intrång, avskräcka, hindra och avslöja handlingar i fråga om interna hot, möjliggöra olika behandling av personalen med avseende på tillgång till Natos säkerhetsklassificerade information utifrån deras intyg över personalsäkerhetsgodkännande och principen om behovsenlig behörighet samt möjliggöra att alla säkerhetsincidenter kan upptäckas och åtgärdas så snart som möjligt.

Fysiska säkerhetsprogram ska grunda sig på principen om skydd på flera nivåer och omfatta en lämplig kombination av kompletterande fysiska säkerhetsåtgärder som ger den nivå av skydd som uppfyller de krav som hänger samman med hur väsentlig och sårbar organisationen och dess information är. De fysiska säkerhetsåtgärderna ska stödjas genom lämpliga åtgärder för personal-, informations-, kommunikations- och informationssystemsäkerhet.

Permanenta eller tillfälliga utrymmen där information i säkerhetsklass NATO CONFIDENTIAL lagras, hanteras eller diskuteras ska organiseras och struktureras så att de motsvarar kraven för Natos säkra utrymme av klass I eller Natos säkra utrymme av klass II. En administrativ zon ska upprättas runt eller leda till Natos säkra utrymmen av klass I eller II. I administrativa zoner får endast information i säkerhetsklass NATO RESTRICTED lagras, hanteras eller diskuteras. Utrymmen av detta slag ska ha en tydlig yttre gräns vid vilken det finns möjlighet att kontrollera personer och fordon.

Permanenta eller tillfälliga tekniskt säkra utrymmen är utrymmen som uttryckligen identifierats kräva skydd mot tekniska angrepp och avlyssning. Dessa utrymmen ska vara föremål för regelbundna fysiska och tekniska inspektioner, och tillträde till dem ska vara strikt kontrollerat.

Information i säkerhetsklasserna COSMIC TOP SECRET, NATO SECRET och NATO CONFIDENTIAL ska lagras i ett säkert utrymme av klass I eller II med iakttagande av de närmare villkor som anges i Natos säkerhetsbestämmelser. Information i säkerhetsklass NATO RESTRICTED ska lagras i ett låst skåp eller en låst kontorsmöbel inom en administrativ zon eller ett säkert utrymme av klass I eller II.

Natos medlemsstater ska använda endast sådan utrustning som den behöriga säkerhetsmyndigheten har godkänt för lagring av Natos säkerhetsklassificerade information.

Bilaga E – Säkerhet när det gäller Natos säkerhetsklassificerade information

I bilaga E till säkerhetsbestämmelserna beskrivs strategin och miniminormerna för säkerheten när det gäller Natos säkerhetsklassificerade information. Informationssäkerhet är vidtagande av allmänna skyddsåtgärder och tillämpning av skyddsförfaranden för att förhindra, upptäcka och klara av förlust eller läcka av säkerhetsklassificerad information.

Upphovsmannen ansvarar för att fastställa säkerhetsklassen av den säkerhetsklassificerade informationen. Enligt en central princip får säkerhetsklassen inte ändras eller sänkas och beslut om att informationen inte ska vara säkerhetsklassificerad inte fattas utan upphovsmannens samtycke. I bilaga E förtecknas Natos säkerhetsklasser, de förkortningar som används för dem samt definieras deras betydelser enligt följande:

COSMIC TOP SECRET (CTS) - obehörigt utlämnande skulle orsaka Nato exceptionellt allvarlig skada, NATO SECRET (NS) - obehörigt utlämnande skulle orsaka Nato allvarlig skada, NATO CONFIDENTIAL (NC) obehörigt utlämnande skulle skada Natos intressen, och NATO RESTRICTED (NR) - obehörigt utlämnande skulle vara icke önskvärt för Natos intressen.

I bilagan fastställs också de avtal och bestämmelser som tillämpas i fråga om de särskilda kategorierna ”ATOMAL”, ”SIOP”, ”CRYPTO” och ”BOHEMIA”.

Information som klassificerats som COSMIC TOP SECRET, NATO SECRET och ATOMAL ska enligt bilaga E omfattas av ansvarsskyldighet. Det ska finnas ett registreringssystem som ansvarar för mottagande, registrering, hantering, distribution och utplåning av den information som omfattas av ansvarsskyldighet. Information i säkerhetsklasserna NATO CONFIDENTIAL

och NATO RESTRICTED behöver inte registreras i registreringssystemet, utom om det föreskrivs i nationella lagar och andra författningar. De organisationer som hanterar information i säkerhetsklass COSMIC TOP SECRET ska utse en COSMIC-tjänsteman.

I bilagan definieras säkerhetsincident, säkerhetsöverträdelse, läcka och förseelse. Alla säkerhetsöverträdelser eller eventuella säkerhetsöverträdelser ska omedelbart rapporteras till den behöriga säkerhetsmyndigheten. Den nationella eller utsedda säkerhetsmyndigheten eller chefen för det berörda militära eller civila Natoorganet rapporterar om bedömning av skadan och om åtgärder för att minimera skadan till Natos säkerhetsbyrå. NOS kan begära att de behöriga myndigheterna gör ytterligare utredningar och rapporterar sina upptäckter till Natos säkerhetsbyrå. NOS kan även informera Natos säkerhetskommitté om detta.

Bilaga F – Säkerhet i kommunikations- och informationssystem

I bilaga F anges strategin och miniminormerna för skydd av Natos säkerhetsklassificerade information samt de systemtjänster och resurser som stöder den i kommunikationen, lagring av denna information i informationssystem och andra elektroniska system samt behandling och överföring av den i dessa system (säkerhet i kommunikations- och informationssystem). I bilagan beskrivs säkerhetsmålen i fråga om informationens konfidentialitet, fullständighet, tillgänglighet, autenticitet och oavvislighet. När industrienheter hanterar säkerhetsklassificerad information på basis av kontrakt tillämpas dessutom särskilda industrisäkerhetsåtgärder (se bilaga G).

Alla nationella kommunikations- och informationssystem i vilka Natos säkerhetsklassificerade information hanteras ska genomgå en säkerhetsackreditering som visar att säkerhetsmålen uppfylls. Genom säkerhetsackreditering kan det konstateras att en lämplig skyddsnivå har uppnåtts och upprätthålls.

I bilaga F förtecknas lämpliga säkerhetsåtgärder som ska tillämpas på alla kommunikations- och informationssystem i vilka man hanterar Natos säkerhetsklassificerade information i syfte att uppnå säkerhetsmålen för skyddet av informationen och de systemtjänster och resurser som stöder den. Genom hantering av säkerhetsrisker när det gäller Natos kommunikations- och informationssystem säkerställs en ständig utvärdering av systemets sårbarheter och överensstämmelse med säkerhetskraven.

När Natos säkerhetsklassificerade information överförs elektroniskt ska särskilda åtgärder vidtas för att säkerhetsmålen ska uppnås vid överföringen. Konfidentialiteten för information i säkerhetsklass NATO SECRET och högre ska vid överföringen av information skyddas med kryptoprodukter och krypteringsmetoder som godkänts av Natos militära kommitté. Konfidentialiteten för information i säkerhetsklass NATO CONFIDENTIAL eller NATO RESTRICTED ska vid överföringen av information skyddas med antingen kryptoprodukter eller krypteringsmetoder som godkänts av Natos militära kommitté eller en medlemsstat i Nato.

I bilagan beskrivs vilka uppgifter som hör till den nationella säkerhetsmyndigheten för kommunikation- och informationssystem (NCSA), den nationella distributionsmyndighet som ansvarar för hanteringen av Natos kryptomaterial och ackrediteringsmyndigheterna.

Bilaga G – Säkerhetsklassificerade projekt och industrisäkerhet

I bilaga G beskrivs strategin och miniminormerna för säkerheten när det gäller Natos säkerhetsklassificerade information inom industrin. Med industrisäkerhet avses tillämpning av skyddsåtgärder och skyddsförfaranden för att förhindra, upptäcka och klara av förlust eller läcka av sä-

kerhetsklassificerad information som industrin hanterar på basis av kontrakt. Natos säkerhetsklassificerade information som sprids till industrin, som produceras som ett resultat av kontrakt som ingås med industrin och kontrakt som ingås med industrin ska skyddas i enlighet med Natos säkerhetsstrategi och dess stödjande direktiv. Entreprenören och underentreprenörerna förutsätts förbinda sig till alla åtgärder som de nationella säkerhetsmyndigheterna eller de utsedda säkerhetsmyndigheterna bestämmer för att skydda säkerhetsklassificerad information som produceras av entreprenören eller av Nato. Bilagan innehåller separata bestämmelser om kontrakt som ingås med entreprenörer i stater som inte hör till Nato.

Den nationella säkerhetsmyndigheten eller de utsedda säkerhetsmyndigheterna i varje medlemsstat i Nato ansvarar för att säkerställa att de enheter som omfattas av dess behörighet och som behöver tillgång till information i säkerhetsklass NATO CONFIDENTIAL och högre har vidtagit nödvändiga skyddsåtgärder för att få ett intyg över säkerhetsgodkännande av verksamhetsställe (Facility Security Clearance, FSC). Entreprenörers anställda som behöver tillgång till Natos information i säkerhetsklass NATO CONFIDENTIAL och högre ska ha ett relevant personalsäkerhetsgodkännande.

Bilaga G innehåller bestämmelser också om kontrollförfaranden för internationella besök, om personal som lånats ut till Natoprojekt eller Natoprogram samt om säkerhetsstrategier som tillämpas på internationell överföring och transport av Natos säkerhetsklassificerade material.

Bilaga H – Säkerhet i förbindelserna med enheter som inte hör till Nato

I bilaga H till säkerhetsbestämmelserna beskrivs strategin och miniminormerna för skydd av Natos säkerhetsklassificerade information som lämnas ut till eller finns tillgänglig för stater som inte hör till Nato och andra organ som inte hör till Nato (till exempel internationella organisationer). Ytterligare detaljer och krav för skydd av Natos säkerhetsklassificerade information som lämnas ut till eller finns tillgänglig för enheter som inte hör till Nato finns i den anvisning om säkerheten i förbindelserna med enheter som inte hör till Nato, som stöder Natos säkerhetsstrategi.

Delning av Natos säkerhetsklassificerade information med enheter som inte hör till Nato ska i princip ske i samband med Natos samarbetsverksamhet som godkänts av Nordatlantiska rådet, men i undantagsfall kan delningen ske också utanför sådan verksamhet.

Innan Natos säkerhetsklassificerade information delas med en enhet som inte hör till Nato ska enheten och Nato ha ingått ett säkerhetsavtal. Säkerhetsstrategierna i säkerhetsavtalet stöds genom en lämplig helhet av administrativa arrangemang. Om inget säkerhetsavtal har ingåtts och det ändå är nödvändigt att utbyta information i rätt tid har en säkerhetsgaranti getts.

De särskilda bestämmelserna om skydd av Natos säkerhetsklassificerade information som lämnas ut till eller finns tillgänglig för enheter som inte hör till Nato gäller personalsäkerhet, fysisk säkerhet, datamaterialsäkerhet, utlämnande myndigheter, registerföring av utlämnade uppgifter samt säkerhet i kommunikations- och informationssystem. I bilaga H anges också de krav som ställs på behandlingen av säkerhetsincidenter.

Ordlista

Som bilaga till säkerhetsbestämmelserna finns också en ordlista med definitioner av de centrala termer som används i bestämmelserna.

De viktigaste förändringarna jämfört med nuläget

Finland tillämpar redan för närvarande Natos säkerhetsbestämmelser C-M(2002)49-REV1 med stöd av det administrativa arrangemanget från 2012. Det att Finland förbinder sig till Natos informationssäkerhetsavtal medför således ingen avsevärd förändring i jämförelse med nuläget. För närvarande har de finländska myndigheterna stöd av tolkningsanvisningen AC/35-D/1038, ”Supporting Document on the Security Protection of NATO Information Released to Non-NATO Nations and International Organisations”, som är avsedd att användas av säkerhetsmyndigheterna i länder som inte är medlemmar i Nato. Utlämnande av Natos säkerhetsklassificerade information till Finland som ett land som inte hört till Nato har i sinom tid förutsatt en särskild formell försäkran från Natos säkerhetsbyrå via certifieringsprocessen för genomförandet av säkerhetsavtalet om att informationen skyddas i Finland i enlighet med minimistandarderna i Natos säkerhetsstrategi.

Inom partnerskapet för fred har tillgången till Nato-handlingar alltid grundat sig på ett skriftligt samtycke av upphovsmannen till informationen, på ett samarbete som godkänts av NAC eller på Finlands deltagande i Natos verksamhet med stöd av NAC. Skillnaden jämfört med nuläget är också att Finland som medlem i Nato kan få handlingar av högsta säkerhetsklass COSMIC TOP SECRET, som i regel inte lämnas ut till länder som inte hör till Nato. Till vissa delar är kraven på hantering av säkerhetsklassificerad information flexiblare för Natoländernas del. Exempelvis är registreringen av NATO CONFIDENTIAL- och NATO RESTRICTED-handlingar beroende av den nationella lagstiftningen. I och med Natomedlemskapet gör Natos säkerhetsbyrå regelbundet *inspektioner* i Finland av säkerhetsåtgärderna för skydd av Natos säkerhetsklassificerade information. Under partnerskapet för fred har Natos säkerhetsbyrå gjort så kallade *inspektionsbesök* till Finland.

För skydd av Natos säkerhetsklassificerade information ska godkända kryptoprodukter användas. Skyddet av uppgifter i säkerhetsklasserna NATO SECRET och COSMIC TOP SECRET förutsätter användning av en kryptoprodukt som godkänts av Natos militära kommitté (NAMILCOM, NATO Military Committee). För skydd av uppgifter i säkerhetsklasserna NATO CONFIDENTIAL och NATO RESTRICTED kan också användas nationella kryptoprodukter som godkänts av medlemsstatens NCSA-myndighet. I och med medlemskapet kan Transport- och kommunikationsverket bedöma och godkänna nationella kryptoprodukter för att skydda uppgifter i säkerhetsklasserna NC och NR.

9 Det administrativa arrangemanget för skydd av säkerhetsklassificerad information som utbyts mellan Finland och Nordatlantiska fördragsorganisationen samt överenskommelsen med Nordatlantiska fördragsorganisationen om informationssäkerhet

Genom 1994 års överenskommelse med Nordatlantiska fördragsorganisationen förband sig Finland att klassificera och skydda det material som erhålls av Nato inom ramen för programmet för partnerskap för fred och att göra säkerhetsutredningar av dem som har tillgång till skyddat material. Till överenskommelsen hade det fogats en redogörelse för den säkerhetsklassificering av handlingar som Nato tillämpar och för vissa administrativa arrangemang som behöver vidtas för genomförandet av överenskommelsen.

År 2012 ingick Finland med Nordatlantiska fördragsorganisationen ett administrativt arrangemang för skydd av säkerhetsklassificerad information, som kompletterade överenskommelsen. I arrangemanget föreskrivs det om säkerhetsmyndigheter, tillämpliga definitioner, märkning, skydd och användning av säkerhetsklassificerad information, tillgång till säkerhetsklassificerad information, förmedling av säkerhetsklassificerad information, immateriella rättigheter, detaljer

i säkerhetskraven, iakttagande av arrangemanget samt säkerhetskontroller, besök, kontrollbesök, försvunnen information eller äventyrande av information, kostnader, tvistlösning samt sedvanliga slutbestämmelser.

När Finland ansluter sig till Nato ska det också ansluta sig till 1997 års avtal mellan parterna i nordatlantiska fördraget om informationssäkerhet, vars bestämmelser ersätter överenskommelsen från 1994 och arrangemanget från 2012. Överenskommelsen och arrangemanget innehåller ingen bestämmelse om uppsägning av dem, men det har förts diskussioner med Nato om överenskommelsens och arrangemangets upphörande i enlighet med artikel 54 b i Wienkonventionen (FördrS 32 och 33/1980). Avsikten är således att säga upp överenskommelsen och arrangemanget och att upphäva lagen om sättande i kraft av dem. Enligt 15 § i lagen om internationella förpliktelser som gäller informationssäkerhet ska bestämmelserna om åtgärder som gäller informationssäkerhet 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.

10 Specialmotivering till lagförslagen

10.1 Lagen om avtalet mellan parterna i nordatlantiska fördraget om informationssäkerhet samt säkerhetsbestämmelserna

1 §. Paragrafen innehåller en sedvanlig blankettlagsbestämmelse, enligt vilken de bestämmelser som hör till området för lagstiftningen i avtalet och i de säkerhetsbestämmelser som antagits med stöd av avtalet, sådana de lyder ändrade i handlingen C-M(2002)49-REV-1 av den 20 november 2020, ska gälla som lag, sådana som Finland har förbundit sig till dem. De bestämmelser i avtalet och i säkerhetsbestämmelserna som hör till området för lagstiftningen behandlas närmare i avsnittet om behovet av riksdagens samtycke.

2 §. Paragrafen innehåller en sedvanlig blankettlagsbestämmelse som gäller sättande i kraft av de bestämmelser i avtalet och i säkerhetsbestämmelserna som inte hör till området för lagstiftningen genom förordning av statsrådet.

3 §. Paragrafen innehåller en sedvanlig blankettlagsbestämmelse enligt vilken bestämmelser om ikraftträdandet av lagen utfärdas genom förordning av statsrådet. Man behöver föreskriva om ikraftträdandet genom förordning för att lagen ska träda i kraft samtidigt som avtalet träder i kraft för Finlands del.

10.2 Lagen om upphävande av lagen om sättande i kraft av de bestämmelser som hör till området för lagstiftningen i det administrativa arrangemanget för skydd av säkerhetsklassificerad information som utbyts mellan Finland och Nordatlantiska fördragsorganisationen samt i överenskommelsen med Nordatlantiska fördragsorganisationen om informationssäkerhet

1 §. Med stöd av 1 § upphävs lagen om sättande i kraft av de bestämmelser som hör till området för lagstiftningen i det administrativa arrangemanget för skydd av säkerhetsklassificerad information som utbyts mellan Finland och Nordatlantiska fördragsorganisationen samt i överenskommelsen med Nordatlantiska fördragsorganisationen om informationssäkerhet (945/2012).

2 §. Bestämmelser om ikraftträdandet av lagen utfärdas genom förordning av statsrådet. Avsikten är att lagen ska sättas i kraft samtidigt som uppsägningen av arrangemanget och överenskommelsen träder i kraft.

11 Ikraftträdande

Avtalet mellan parterna i nordatlantiska fördraget om informationssäkerhet träder för Finlands del i kraft trettio dagar efter den dag då Finland deponerar sitt anslutningsinstrument för avtalet hos Amerikas förenta staters regering. Det föreslås att den lag om sättande i kraft av avtalet som ingår i propositionen ska träda i kraft samtidigt som avtalet träder i kraft för Finlands del, vid en tidpunkt som föreskrivs genom förordning av statsrådet.

Avsikten är att uppsägningen av det administrativa arrangemanget för skydd av säkerhetsklassificerad information som utbyts mellan Finland och Nordatlantiska fördragsorganisationen samt överenskommelsen om informationssäkerhet med Nordatlantiska fördragsorganisationen ska träda i kraft samtidigt som Finlands anslutning till avtalet mellan parterna i Nordatlantiska fördragsorganisationen om informationssäkerhet träder i kraft. Det föreslås att den i propositionen ingående lagen om upphävande av lagen om sättande i kraft av de bestämmelser som hör till området för lagstiftningen i dessa fördrag träder i kraft samtidigt som uppsägningen av fördragen träder i kraft, vid en tidpunkt som föreskrivs genom förordning av statsrådet.

12 Bifall av Ålands lagting

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

Avtalet mellan parterna i nordatlantiska fördraget om informationssäkerhet innehåller inga bestämmelser som faller inom landskapet Ålands behörighet och förutsätter således inte landskapets bifall i enlighet med 59 § i självstyrelselagen för Åland.

Enligt självstyrelselagen behövs lagtingets bifall inte för uppsägning av ett avtal eller för en lag om upphävande av lagen om sättande i kraft av ett avtal.

13 Förhållande till andra propositioner

Denna regeringsproposition har samband med regeringens proposition om godkännande och sättande i kraft av nordatlantiska fördraget och avtalet om status för Nordatlantiska fördragsorganisationen, nationella representanter och organisationens internationella personal (RP 315/2022 rd), som överlämnades till riksdagen den 5 december 2022. Finland har vid anslutningsförhandlingarna förbundit sig att ansluta sig till Natos informationssäkerhetsavtal inom 12 månader från deponeringen av Finlands anslutningsinstrument för nordatlantiska fördraget.

Bestämmelser om informationssäkerhet finns också i Natos avtal om ömsesidigt säkerställande av sekretess för försvarsrelaterade uppfinningar för vilka patent sökts, i Natos avtal om överföring av teknisk information för försvarsändamål samt i avtalet mellan parterna i nordatlantiska fördraget om samarbete avseende nukleär information. Separata regeringspropositioner lämnas om godkännandet av dessa avtal.

En separat regeringsproposition lämnas också för godkännande av avtalet mellan parterna i Nordatlantiska fördraget om status för deras styrkor (Nato SOFA) och av protokollet om status för de internationella militära högkvarter som inrättats enligt nordatlantiska fördraget (Parisprotokollet).

14 Behovet av riksdagens samtycke samt behandlingsordning

14.1 Behovet av riksdagens samtycke

Avtalet mellan parterna i nordatlantiska fördraget om informationssäkerhet

Enligt 94 § 1 mom. i grundlagen krävs riksdagens godkännande för fördrag och andra internationella förpliktelser som innehåller sådana bestämmelser som hör till området för lagstiftningen eller annars har avsevärd betydelse, eller som enligt grundlagen av någon annan anledning kräver riksdagens godkännande. Riksdagens godkännande krävs också för uppsägning av en sådan förpliktelse. Enligt grundlagsutskottets tolkningspraxis ska en bestämmelse anses höra till området för lagstiftningen om den gäller utövande eller begränsning av någon grundläggande frieller rättighet som är skyddad i grundlagen, om den i övrigt gäller grunderna för individens rättigheter och skyldigheter, om den sak som bestämmelsen gäller är sådan att om den enligt grundlagen ska föreskrivas i lag eller om det finns lagbestämmelser om den sak som bestämmelsen gäller eller om det enligt rådande uppfattning i Finland ska lagstiftas om saken. Grundlagsutskottet har ansett att en bestämmelse i en internationell förpliktelse på dessa grunder hör till området för lagstiftningen oavsett om den strider mot eller överensstämmer med en lagbestämmelse i Finland (GrUU 11/2000 rd och GrUU 12/2000 rd).

I artikel 1 punkt i i avtalet definieras, tillsammans med bilagorna I och II, vad som avses med säkerhetsklassificerad information som ska skyddas. Eftersom definitionen direkt eller indirekt påverkar tolkningen och tillämpningen av materiella bestämmelser i avtalet som hör till området för lagstiftningen kräver artikel 1 punkt i samt bilagorna I och II riksdagens godkännande (GrUU 6/2001 rd).

I artikel 1 punkterna ii och iii i avtalet föreskrivs det om åtgärder som krävs för att skydda säkerhetsklassificerad information inom tillämpningsområdet för avtalet och som begränsar utlämnande och användning av informationen. I artikeln är det fråga om en med tanke på avtalet väsentlig bestämmelse med stöd av vilken Finland kan skydda sådan säkerhetsklassificerad information som avses i avtalet utan den skaderekvisitbedömning som föreskrivs i offentlighetslagen. Bestämmelsen hör till området för lagstiftningen.

Enligt artikel 2 i avtalet ska parterna säkerställa att en nationell säkerhetsmyndighet, som ska vidta skyddande säkerhetsåtgärder, inrättas för Natos verksamhet. I 4 § i lagen om internationella förpliktelser som gäller informationssäkerhet finns bestämmelser om Finlands nationella säkerhetsmyndighet och utsedda säkerhetsmyndigheter och om deras befogenheter. Den i artikeln föreskrivna skyldigheten att ha en nationell säkerhetsmyndighet hör till området för lagstiftningen.

Enligt artikel 2 i avtalet ska parterna utarbeta och tillämpa säkerhetskrav, som ska säkerställa en gemensam skyddsnivå för säkerhetsklassificerad information. Artikeln utgör en rättslig grund för de bestämmelser och direktiv som gäller skydd av Natos säkerhetsklassificerade information och som Finland förbinder sig att iaktta efter att ha anslutit sig till Nato. I artikeln delegeras behörigheten att ingå avtal om säkerhetskrav till Nordatlantiska rådet. Bestämmelsen om delegering hör till området för lagstiftningen.

I artikel 3 i avtalet föreskrivs det om parternas skyldighet att säkerställa att alla som i sina arbetsuppgifter behöver eller kan komma att få tillgång till information i säkerhetsklass CONFIDENTIAL eller högre genomgår en relevant säkerhetsutredning. Artikeln innehåller bestämmelser om kvarstående risk i samband med säkerhetsutredningsförfaranden och om samarbete

mellan parterna. I Finland finns bestämmelser om vilka personer som är föremål för säkerhetsutredningar och om utredningsförfarandet i säkerhetsutredningslagen. Artikel 3 i avtalet innehåller bestämmelser som hör till området för lagstiftningen.

Natos säkerhetsbestämmelser

De viktigaste principerna och miniminormerna för säkerhet i Natos säkerhetsstrategi ingår i Natos säkerhetsbestämmelser C-M(2002)49-REV1, som godkänts av Nordatlantiska rådet (NAC). Det är inte brukligt att nationellt sätta i kraft säkerhetsstrategier som antagits med stöd av internationella överenskommelser om informationssäkerhet. Natos säkerhetsbestämmelser innehåller dock nedan uppräknade bestämmelser som hör till området för lagstiftningen och som inte direkt framgår av texten i informationssäkerhetsavtalet. För sådana bestämmelser anses det nödvändigt att begära riksdagens godkännande och sätta dem i kraft nationellt (GrUU 19/2010 rd, s. 5). Texten i säkerhetsbestämmelserna finns som bilaga till regeringspropositionen.

Bilaga A till säkerhetsbestämmelserna innehåller texten till det egentliga informationssäkerhetsavtalet, och de bestämmelser i den som hör till området för lagstiftningen redogörs det för ovan.

Punkt 1 (b) i bilaga B till säkerhetsbestämmelserna innehåller en grundläggande princip om behovet av information (need-to-know). Bestämmelser om detta finns i 6 § 3 mom. i lagen om internationella förpliktelser som gäller informationssäkerhet. I punkt 3 i bilagan definieras den nationella säkerhetsmyndighetens uppgifter och i punkt 5 i bilagan förutsätts det att varje medlemsstat i Nato har en utsedd säkerhetsmyndighet som ansvarar för genomförandet av bestämmelserna om industrisäkerhet. Bestämmelser om Finlands säkerhetsmyndigheter och deras uppgifter finns i 4 § i lagen om internationella förpliktelser som gäller informationssäkerhet. I punkt 9 (f) i bilagan ges Natos säkerhetsbyrå i uppgift att också i medlemsstaterna utföra regelbundna säkerhetsinspektioner för skydd av Natos säkerhetsklassificerade information. Bestämmelser om besök av representanter för internationella organ för utförande av säkerhetsinspektioner finns i 18 § i lagen om internationella förpliktelser som gäller informationssäkerhet.

I punkt 7 i bilaga C till säkerhetsbestämmelserna definieras personer i hög statlig ställning, till exempel stats- och regeringschefer, ministrar samt parlaments- och domstolsledamöter, i fråga om vilka behovet av säkerhetsutredning av person bestäms i enlighet med nationell lagstiftning och nationella bestämmelser. Också dessa grupper av personer ska behöva informationen och informeras om sina säkerhetsförpliktelser.

I punkt 6 i bilaga E till säkerhetsbestämmelserna anges Natos säkerhetsklasser och hur de ska märkas ut. I punkterna 32–39 i bilagan definieras säkerhetsincident, säkerhetsöverträdelse, läcka och förseelse samt utrednings- och rapporteringsskyldigheter i anslutning till dessa. Bestämmelser om utredning av och anmälan om förseelser finns i 19 § i lagen om internationella förpliktelser som gäller informationssäkerhet.

Bilaga F till säkerhetsbestämmelserna innehåller bestämmelser om datamaterialsäkerhet. Punkt 3 i bilaga F till säkerhetsbestämmelserna gäller skyldigheten att ackreditera informationssystem. Bestämmelser om bedömning av informationssystem finns i lagen om bedömning av informationssäkerheten i myndigheternas informationssystem och datakommunikation. Enligt 8 a § i den lagen får det genom förordning av statsrådet föreskrivas att ett intyg som avses i 8 § ska skaffas i fråga om informationssystem eller datakommunikation som en statsförvaltningsmyndighet bestämmer över och där handlingar som hör till säkerhetsklass I eller II behandlas. Punkt 13.4 i bilagan gäller NCSA:s uppgifter. Bestämmelser om Finlands säkerhetsmyndigheter och

deras uppgifter finns i 4 § i lagen om internationella förpliktelser som gäller informationssäkerhet, enligt vilken Transport- och kommunikationsverket är den nationella säkerhetsmyndighetens sakkunniga i ärenden som gäller informationssäkerhet i fråga om informationssystem och datakommunikation.

Punkt 4 i bilaga G till säkerhetsbestämmelserna innehåller ett krav på ett intyg över säkerhetsutredning av företag som hanterar information i säkerhetsklass CONFIDENTIAL eller högre. Punkt 10 i bilagan innehåller en avtalsförpliktelse för företag att skydda säkerhetsklassificerad information. Bestämmelser om säkerhetsutredningar av företag finns i 5 kap. i säkerhetsutredningslagen och i 12 § i lagen om internationella förpliktelser som gäller informationssäkerhet.

14.2 Behandlingsordning

I avtalet mellan parterna i nordatlantiska fördraget om informationssäkerhet definieras Natos regler om informationssäkerhet, som Natos medlemsstater ska iaktta när de behandlar säkerhetsklassificerad information. Det är fråga om särskilda bestämmelser i förhållande till den allmänna lagstiftning som gäller offentligheten för de nationella myndigheternas handlingar. Enligt 12 § i grundlagen är myndigheternas handlingar offentliga, om inte offentligheten av tvingande skäl särskilt har begränsats genom lag. Informationssäkerhetsavtalet innehåller sådana i 12 § i grundlagen avsedda bestämmelser genom vilka offentligheten begränsas av tvingande skäl.

Internationella överenskommelser om informationssäkerhet är ett etablerat sätt att reglera utbytet av säkerhetsklassificerad information mellan Finland och någon annan stat eller internationell organisation. Finland har för närvarande sammanlagt 26 gällande överenskommelser om informationssäkerhet som riksdagen har godkänt med enkel majoritet och behandlat lagarna om sättande i kraft av dem i vanlig lagstiftningsordning. Grundlagsutskottet har i sitt utlåtande GrUU 39/1997 rd vid behandlingen av säkerhetsskyddsavtalet mellan Finland och Västeuropeiska unionen (VEU) (inte längre gällande) ansett att en begränsning av offentlighetsprincipen på det sätt som avses i avtalet och 2 § i lagen om ikraftträdande kunde anses nödvändig med tanke på att göra det möjligt för Finland att samarbeta med VEU. Sekretessintresset svarade också mot de grunder som nämndes i 9 § i den då gällande lagen om allmänna handlingars offentlighet (83/1951). Lagen om ikraftträdande av avtalet kunde behandlas i vanlig lagstiftningsordning. Efter detta har, också i vanlig lagstiftningsordning, stiftats lagen om internationella förpliktelser som gäller informationssäkerhet, i vilken det föreskrivs om myndigheternas åtgärder för att uppfylla internationella förpliktelser som gäller informationssäkerhet.

Det administrativa arrangemanget mellan Finland och Nato för skydd av säkerhetsklassificerad information från 2012 har godkänts med enkel majoritet och lagen om sättande i kraft av arrangemanget har stiftats i vanlig lagstiftningsordning. Samtidigt sattes de bestämmelser i den 1994 ingångna överenskommelsen mellan Finland och Nato som hör till området för lagstiftningen i kraft i vanlig lagstiftningsordning. Enligt regeringens proposition breddade bestämmelserna i artikel 5 i det administrativa arrangemang som lämnats till riksdagen för godkännande inte skyldigheten att iaktta sekretess från vad som reglerades i 6 § i lagen om internationella förpliktelser som gäller informationssäkerhet (RP 139/2012 rd).

Genom det aktuella informationssäkerhetsavtalet förbinder man sig att iaktta motsvarande förpliktelser som gäller informationssäkerhet och som Finland redan har förbundit sig till genom överenskommelsen om informationssäkerhet från 1994 och det administrativa arrangemanget från 2012. Förpliktelserna i informationssäkerhetsavtalet kan anses vara nödvändiga begränsningar av offentligheten för att möjliggöra det samarbete som avses i nordatlantiska fördraget.

Enligt artikel 2 i det avtal som nu ska godkännas ska parterna utarbeta och tillämpa säkerhetskrav, som ska säkerställa en gemensam skyddsnivå för säkerhetsklassificerad information. Ovan i avsnitt 8.2 beskrivs dessa bestämmelser om genomförandet av informationssäkerhetsavtalet. I säkerhetsstrategin är det juridiskt sett fråga om tekniska bestämmelser som tryggar genomförandet av informationssäkerhetsavtalet.

Finlands grundlag har 2012 ändrats så att enligt bestämmelserna i grundlagens 94 § 2 mom. och 95 § 2 mom. ska beslut som med hänsyn till Finlands suveränitet gäller *betydande* överföring av behörighet till Europeiska unionen eller till en internationell organisation eller institution godkännas med minst två tredjedelar av de avgivna rösterna. Däremot är det möjligt att med enkel majoritet besluta om godkännande och ikraftträdande av internationella förpliktelser som innebär överföring av annan än betydande behörighet.

I den regeringsproposition som gällde en ändring av grundlagen konstateras det att det vid överföring av riksdagens behörighet vanligen är fråga om sådana internationella avtalsarrangemang där lagstiftningsmakt bara i liten omfattning överförs på en internationell institution i frågor av teknisk natur eller inom mycket begränsade områden, och att beslut om överföring av sådan behörighet framdeles ska kunna fattas med enkel majoritet (RP 60/2010 rd, s. 27).

I artikel 2 i avtalet delegeras behörigheten att ingå avtal om säkerhetskrav till Nordatlantiska rådet. Det är dock inte fråga om en med tanke på suveränitetsbestämmelserna i grundlagen betydande delegering av behörighet, utan om utfärdande av sådana närmare bestämmelser om genomförandet av avtalet som är sedvanliga i modern internationell samverkan och om vilka parterna i nordatlantiska fördraget enhälligt beslutar. Bestämmelserna om informationssäkerhet tillämpas i huvudsak av myndigheterna. För företag har de betydelse om företagen ingår ett säkerhetsklassificerat kontrakt som inbegriper behandling av Natos säkerhetsklassificerade information. För enskilda personer har avtalet och informationssäkerhetsstrategin närmast indirekt betydelse.

Grundlagsutskottet har ansett att det inte har varit ett problem att utfärda tillämpningsföreskrifter av teknisk natur som hör till området för lagstiftningen, men till den del de har hört till området för lagstiftningen har utskottet i regel förutsatt att de sätts i kraft och publiceras (GrUU 19/2010 rd, s. 5). Natos säkerhetsbestämmelser i handlingen C-M(2002)49-REV1 innehåller vissa bestämmelser som hör till området för lagstiftningen, som beskrivs ovan i avsnitt 14.1 och som inte framgår direkt av texten till informationssäkerhetsavtalet. För sådana bestämmelser begärs riksdagens godkännande, de har tagits in i lagen om sättande i kraft av avtalet, och säkerhetsbestämmelserna publiceras tillsammans med Natos informationssäkerhetsavtal i Finlands författningssamlings fördragsserie. I fortsättningen publiceras ändringar i säkerhetsbestämmelserna genom ett meddelande i fördragsserien i enlighet med 9 § 2 mom. i lagen om Finlands författningssamling (188/2000).

Eftersom avtalet mellan parterna i nordatlantiska fördraget om informationssäkerhet och säkerhetsbestämmelserna inte innehåller bestämmelser som gäller grundlagen på det sätt som avses i 94 § 2 mom. eller 95 § 2 mom. i grundlagen, kan avtalet och säkerhetsbestämmelserna enligt regeringens uppfattning godkännas med enkel majoritet och förslaget till lag om sättande i kraft av dem godkännas i vanlig lagstiftningsordning.

Enligt grundlagsutskottets och utrikesutskottets ståndpunkt kan beslut om uppsägning av en internationell förpliktelse fattas med enkel majoritet (GrUB 10/1998 rd och UtUU 6/1998 rd). Beslut om godkännande av uppsägningen av det administrativa arrangemanget för skydd av säkerhetsklassificerad information som utbyts mellan Finland och Nordatlantiska fördragsorga-

nisationen samt av överenskommelsen med Nordatlantiska fördragsorganisationen om informationssäkerhet kan fattas med enkel röstmajoritet och lagen om upphävande av lagen om sättande i kraft av de bestämmelser som hör till området för lagstiftningen i fördragen kan godkännas i vanlig lagstiftningsordning.

Kläm 1

Med stöd av vad som anförts ovan och i enlighet med 94 § i grundlagen föreslås det

att riksdagen godkänner det i Bryssel den 6 mars 1997 mellan parterna i nordatlantiska fördraget ingångna avtalet om informationssäkerhet samt de säkerhetsbestämmelser som antagits med stöd av avtalet, sådana de lyder ändrade i handlingen C-M(2002)49-REV1 av den 20 november 2020, och

att riksdagen godkänner uppsägningen av det i Helsingfors den 3 juli 2012 ingångna administrativa arrangemanget för skydd av säkerhetsklassificerad information som utbyts mellan Finland och Nordatlantiska fördragsorganisationen samt av den i Bryssel den 22 september 1994 med Nordatlantiska fördragsorganisationen ingångna överenskommelsen om informationssäkerhet (FördrS 7 och 8/2013).

Kläm 2

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

1.

Lag

om avtalet mellan parterna i nordatlantiska fördraget om informationssäkerhet samt säkerhetsbestämmelserna

I enlighet med riksdagens beslut föreskrivs:

1 §

De bestämmelser som hör till området för lagstiftningen i det i Bryssel den 6 mars 1997 mellan parterna i nordatlantiska fördraget ingångna avtalet om informationssäkerhet samt i de säkerhetsbestämmelser som antagits med stöd av avtalet, sådana de lyder ändrade i handlingen C-M(2002)49-REV1 av den 20 november 2020, ska gälla som lag, sådana som Finland har förbundit sig till dem.

2 §

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

3 §

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

2.

Lag

om upphävande av lagen om sättande i kraft av de bestämmelser som hör till området för lagstiftningen i det administrativa arrangemanget för skydd av säkerhetsklassificerad information som utbyts mellan Finland och Nordatlantiska fördragsorganisationen samt i överenskommelsen med Nordatlantiska fördragsorganisationen om informationssäkerhet

I enlighet med riksdagens beslut föreskrivs:

1 §

Genom denna lag upphävs lagen om sättande i kraft av de bestämmelser som hör till området för lagstiftningen i det administrativa arrangemanget för skydd av säkerhetsklassificerad information som utbyts mellan Finland och Nordatlantiska fördragsorganisationen samt i överenskommelsen med Nordatlantiska fördragsorganisationen om informationssäkerhet (945/2012).

2 §

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

Helsingfors den 20

Statsminister

Förnamn Efternamn

Utrikesminister Förnamn Efternamn