Statsrådets skrivelse till riksdagen om översyn av rådets beslut om säkerhetsbestämmelser för skydd av säkerhetsskyddsklassificerade EU-uppgifter 2013/488/EU (*rådets säkerhetsbestämmelser*)

I enlighet med 96 § 2 mom. i grundlagen översänds till riksdagen en promemoria om översyn av rådets beslut om säkerhetsbestämmelser för skydd av säkerhetsskyddsklassificerade EU-uppgifter.

Helsingfors den14 december 2023

Utrikesminister Elina Valtonen

Utrikesråd Päivi Kaukoranta

ÖVERSYN AV RÅDETS BESLUT OM SÄKERHETSBESTÄMMERLSER FÖR SKYDD AV SÄKERHETSSKYDDSKLASSIFICERADE EU-UPPGIFTER

1 Förslagets bakgrund och syften

Rådets beslut om säkerhetsbestämmelser för skydd av säkerhetsskyddsklassificerade EU-uppgifter (2013/488/EU) trädde i kraft för tio år sedan, den 15 oktober 2013. Några år efter att säkerhetsbestämmelserna trätt i kraft uttryckte medlemsstaterna en önskan om att uppdatera och förenkla säkerhetsbestämmelserna. Ett konceptdokument om översyn av bestämmelserna föredrogs för rådets säkerhetskommitté 2016. Bakom uppdateringsbehovet låg att man i allt högre grad har övergått från pappershandlingar till elektronisk behandling av säkerhetsskyddsklassificerade EU-uppgifter, vilket kräver olika skyddsåtgärder. Möjligheten diskuterades att övergå från preskriptiva anvisningar till en strategi som grundar sig på riskhantering. I säkerhetskommittén föreslogs det att man skulle bereda kriterier för att skydda säkerhetsskyddsklassificerade EU-uppgifter (common core), som skulle gälla även unionens övriga institutioner och organ. Ett långsiktigare mål var att utvidga de gemensamma kriterierna till att gälla även EU:s byråer. Denna strategi strandade på grund av problem gällande den rättsliga grunden och man beslutade i diskussionerna att fokusera på att revidera rådets säkerhetsbestämmelser.

Som ett grundläggande mål för revideringen av rådets säkerhetsbestämmelser angavs att utnyttja erfarenheterna från tillämpningen av bestämmelserna och de inspektioner som utfördes i medlemsstaterna 2019. Syftet var även att utvärdera vilka bestämmelser som inte har tillämpats i praktiken och huruvida säkerhetsbestämmelserna innehåller allt för strikta, lindriga eller otydliga bestämmelser. Som mål angavs även att ändra säkerhetsbestämmelsernas uppbyggnad så att de regler som ingår i de nuvarande bestämmelsernas bilagor överförs till de egentliga artiklarna i rättsakten.

Utöver rådets säkerhetsbestämmelser har man 2011 ingått ett avtal mellan Europeiska unionens medlemsstater, församlade i rådet om skydd av säkerhetsskyddsklassificerade uppgifter som utbyts i Europeiska unionens intresse (FördrS 76 och 77/2015). I artikel 3 åläggs medlemsstaterna att vidta alla lämpliga åtgärder i enlighet med sina respektive nationella lagar och andra författningar för att iaktta rådets säkerhetsbestämmelser. Europeiska unionen har tagit i bruk sådana förfaranden och reglar för behandling av säkerhetsklassificerad information som till stor del påminner om Natos system.

Revideringen av rådets säkerhetsbestämmelser hör samman med kommissionens förslag till Europaparlamentets och rådets förordning om informationssäkerhet i unionens institutioner, organ och byråer (COM(2022) 119 final, se E-brev E141/2022 rd).

2 Förslagets huvudsakliga innehåll

Tills vidare finns inte något övergripande förslag till rådets nya säkerhetsbestämmelser. Utifrån diskussionen i säkerhetskommittén kan man uppskatta, att säkerhetsbestämmelsernas uppbyggnad kommer att ändras och artikelnumreringen förnyas. De bestämmelser som finns i bilagorna till de nuvarande säkerhetsbestämmelserna tas in i beslutets artiklar. Nedan redogörs

för förslagets huvudsakliga innehåll utifrån det tillgängliga materialet på engelska. Andra språkversioner finns inte ännu.

Personalsäkerhet. Eftersom många aspekter i anslutning till personalsäkerheten hör till den nationella behörigheten kommer man i översynen att fokusera på att förenkla vissa regler i säkerhetsbestämmelserna så att man kan skapa gemensamma minimikrav i synnerhet för säkerhetsprövningar. De är i de flesta fall dock frivilliga för medlemsstaterna. Hänvisningen till konformiteten med nationell lagstiftning innebär i detta sammanhang både kriteriernas innehåll och den process som ska iakttas.

Revideringen innehåller mer detaljerade bestämmelser än i dag om förfarandena för att få tillgång till säkerhetsskyddsklassificerade EU-uppgifter. Syftet är att effektivisera åtgärderna för efterhandsövervakning i generalsekretariatet för att öka den allmänna säkerheten. I de nya reglerna ska ”behovet av information” (need-to-know) definieras. Med detta avses att en person har behov av att få tillgång till vissa klassificerade uppgifter för att sköta sina officiella uppgifter eller uppdrag. Avsikten är att förenkla förfarandena för hur representanterna visar sina intyg över personalsäkerhetsgodkännanden (PSC) när de deltar i rådets sekretessbelagda möten. Kravet på utbildning och medvetandegörande när det gäller säkerhet som innebär att säkerhetsutbildning (briefing) ska ges med minst 3 års intervaller ska även gälla de personer som behandlar uppgifter på nivån RESTREINT UE/EU RESTRICTED.

Ett tillfälligt bemyndigande om tillgång till klassificerade uppgifter i en situation där en säkerhetsprövning pågår, förutsätter även i framtiden medverkan av den medlemsstat som utför säkerhetsprövningen. Ett tillfälligt bemyndigande som gäller högst sex månader i taget ska kunna förnyas en gång. Det så kallade ad hoc-bemyndigandet är ett nytt förfarande där generalsekretariatet i undantagsfall kan bevilja en person ett bemyndigande för tillgång till säkerhetsskyddsklassificerade uppgifter. Förfarandet kan tillämpas i situationer där tillfälliga bemyndiganden inte erkänns i medlemsstatens lagstiftning och lagstiftningen inte tillåter att uppgifter lämnas ut innan säkerhetsprövningen slutförts. Bemyndigandet kan förnyas, men ett nytt bemyndigande kan inte beviljas om det har gått 6 månader från det första bemyndigandet som beviljats för undantagsfall. Generalsekretariatet ska därtill meddela medlemsstaten om det ämnar bevilja ett sådant bemyndigande och personen ska ge ett skriftligt bekräftande över att han eller hon förstår reglerna om behandling av klassificerade uppgifter. Ad hoc-bemyndigandet innebär inte heller att man kan avvika från need-to-know-kravet.

Fysisk säkerhet. Med fysisk säkerhet avses fysiska och tekniska säkerhetsåtgärder för att hindra obehörig tillgång till säkerhetsskyddsklassificerade EU-uppgifter. Bland utgångspunkterna vid översynen av bestämmelserna om fysisk säkerhet betonas behovet av att utarbeta en förteckning över de obligatoriska minimikrav som gäller fysisk säkerhet som alla medlemsstater kan samtycka till i stället för att införa flera frivilliga åtgärder. Det var även nödvändigt att se över strategin i fråga om riskhanteringsprincipen. Kraven på fysiskt skyddade områden ska uppdateras i synnerhet med tanke på att man i allt högre grad övergår till elektronisk hantering av säkerhetsskyddsklassificerade EU-uppgifter.

Vid revideringen är det meningen att stärka de obligatoriska minimikraven om fysisk säkerhet på ett tydligare sätt än idag för att även skydda muntliga säkerhetsskyddsklassificerade EU-uppgifter. Den nya bestämmelsen möjliggör dock undantag utifrån en riskbedömning och under förutsättning att undantaget dokumenteras och ett tillräckligt skydd för säkerhetsskyddsklassificerade EU-uppgifter säkerställs. Ramarna för fysiskt skyddade områden och de fysiska säkerhetskraven ska ses över. Indelningen i säkrade utrymmen av klass I (när tillträde till ett säkrat utrymme i praktiken innebär direkt tillgång till de säkerhetsskyddsklassificerade uppgifter som finns där) och klass II (när tillträde till ett säkrat

utrymme i praktiken inte innebär direkt tillgång till de säkerhetsskyddsklassificerade uppgifter som finns där) ska återinföras (jfr. de tidigare säkerhetsbestämmelserna 2001/264/EG). Tekniskt säkrade utrymmen ska definieras som olika säkrade utrymmen som huvudsakligen syftar till att skydda mot avlyssning (sekretessbelagda möten). Kraven på dessa områden ska stärkas (akustiskt skydd, teknisk säkerhetsundersökning (TSCM)).

De krav på anordningar som används för att skydda säkerhetsskyddsklassificerade EU-uppgifter ska specificeras enligt säkerhetsskyddsklassificeringsnivå och kraven på RESTREINT UE/EU RESTRICTED-nivå ska luckras upp. Generalsekretariatet ska ha skyldighet att föra en riktgivande förteckning över de tekniska standarderna och godkända anordningarna för varje nivå. Även kraven på de säkerhetsnycklar och kombinationsinställningar som används för att skydda säkerhetsskyddsklassificerade EU-uppgifter ska specificeras och tillämpas på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL och högre nivåer. I fråga om generalsekretariatets sekretessbelagda möten ska fysiska säkerhetskrav införas.

Hantering av säkerhetsskyddsklassificerade uppgifter. I utredningen har man fokuserat på behovet att omfatta hela livscykeln för säkerhetsskyddsklassificerade EU-uppgifter och ta i beaktande principen om spårbarhet för säkerhetsskyddsklassificerade EU-uppgifter. Andra mål är att registrera säkerhetsskyddsklassificerade EU-uppgifter för säkerhetsändamål och att förenkla och förtydliga de detaljerade bestämmelserna om transport av säkerhetsskyddsklassificerade EU-uppgifter. Bestämmelserna om registrering för säkerhetsändamål ska förenklas genom att man fokuserar på själva registeruppgiften – utförandet av registreringen – i stället för detaljer i genomförandet. Förutom innehavare av säkerhetsskyddsklassificerade EU-uppgifter ska även all tillgång till dessa uppgifter registreras. Kraven på utformning, markering och kopiering av säkerhetsskyddsklassificerade EU-uppgifter ska ses över så att de omfattar uppgifter i alla format (pappersform, elektronisk form eller audio/video).

I de fall där säkerhetsskyddsklassificerade EU-uppgifter lämnas till en tredjestat eller internationell organisation ska de beroende på fall befordras i enlighet med ett informationssäkerhetsavtal eller en administrativ överenskommelse. Säkerhetskommittén ska ge andra än säkerhetsprövade kommersiella kurirtjänster möjlighet att befordra säkerhetsskyddsklassificerade EU-uppgifter (med undantag för säkerhetsskyddsklassificeringsnivån TRÉS SECRET UE/EU TOP SECRET) inom unionens område eller till unionens lokaler i en tredjestats område, och den behöriga myndigheten hos avsändaren beslutar om användningen av dessa tjänster. En ny bestämmelse är att den automatiska skyddsklassificeringen ska upphöra att gälla för sådana säkerhetsskyddsklassificerade EU-uppgifter som har klassificerats som RESTREINT UE/EU RESTRICTED och som härstammar från generalsekretariatet. Det sker 15 år efter att dessa säkerhetskyddsklassificerade EU-uppgifter har skapats. Upphörandet av den automatiska skyddsklassificeringen ska tillämpas endast på den säkerhetsskyddsklassificering som sker efter att de reviderade säkerhetsbestämmelserna träder i kraft. För förstöring och evakuering i nödsituation av säkerhetskyddsklassificerade EU-uppgifter ska det utarbetas anvisningar som fastställer lämpliga förstöringsmetoder och -standarder. För register införs ett krav på att åtminstone varje år göra en förteckning över säkerhetsskyddsklassificerade EU-uppgifter på säkerhetsskyddsklassificeringsnivån CONFIDENTIEL UE/EU CONFIDENTIAL eller högre nivå.

Skydd av säkerhetsskyddsklassificerade EU-uppgifter i kommunikations- och informationssystem (CIS). I den granskade riskhanteringsprincipen hänvisas uttryckligen till en hotbedömning av säkerhetsskyddsklassificerade EU-uppgifter och två pelare: säkerhetsåtgärder

på grundnivå och riskhanteringsåtgärder (extra åtgärder). De främsta ändringsförslagen gäller bland annat ackrediteringsprocessen för CIS, dvs. det föreslås att ackrediteringens roll som ett villkor för att börja behandla uppgifter elektroniskt förtydligas för att minska behovet av tillfälliga beslut om införande (IATO) samt att man ska ingripa i situationer där kraven inte iakttas. Det föreslås att förfarandet för att ackreditera och godkänna produkter utvidgas begränsat även till andra kryptoprodukter. Dessutom föreslås det att myndigheten för informationssäkring (IAA) ges till uppgift att godkänna resultaten av systemspecifika riskbedömningar av de risker på hög nivå som gäller säkerhetsskyddsklassificerade EU-uppgifter. I fråga om den säkra sammankopplingen mellan kommunikations- och informationssystemen ska säkerhetsbestämmelserna kompletteras med en bestämmelse som tydligare än tidigare begränsar sammankopplingen enbart till motiverade behov. Det föreslås även att markeringen och administreringen av lagringsmedier preciseras.

Industrisäkerhet. Det allmänna målet med översynen av bestämmelserna om industrisäkerhet är att stärka skyddet för säkerhetsskyddsklassificerade EU-uppgifter i fråga om säkerhetsskyddsavtal genom att se över och avtala om miniminormer som motsvarar generalsekretariatets behov som upphandlingsmyndighet och som kan genomföras i enlighet med medlemsstaternas nationella regelverk. Syftet med de föreslagna ändringarna är i första hand att se över de krav som gäller de nationella säkerhetsmyndigheterna och de utsedda säkerhetsmyndigheterna och som dessa använder för att bedöma sökandes lämplighet att få en industrisäkerhetsprövning (FSC) och i synnerhet bedöma företagets eller den övriga enhetens pålitlighet. Avsikten är även att behandla de fall där medlemsstaterna inte enligt nationell lagstiftning beviljar FSC till vissa inrättningar. Övriga mål är att stärka de detaljerade åtgärderna för användningen av kommunikations- och informationssystem (CIS) i anslutning till säkerhetsskyddsavtal samt att fastställa specialbestämmelser för de avtal som klassificerats som RESTREINT UE/EU RESTRICTED i synnerhet i de fall där vissa medlemsstater kräver FSC för avtal på denna klassificeringsnivå medan andra inte gör det. En del av översynsarbetet fokuseras på att förenhetliga terminologin i branschen med terminologin i budgetförordningen.

Utbyte av säkerhetsskyddsklassificerade uppgifter med tredjestater och internationella organisationer. Genom översynen strävar man efter att harmonisera och förtydliga de förfaranden som gäller utbyte av säkerhetsskyddsklassificerade uppgifter med tredjestater och internationella organisationer. Även digitaliseringens effekt och det ökade utbytet av information i elektronisk form i anslutning till den ska beaktas. Säkerhetskommitténs roll när det gäller att säkerställa att frågorna om skyddet av säkerhetsskyddsklassificerade uppgifter är enhetliga ska stärkas genom att förbättra informationsgången.

Förfaranden ska införas för att bemyndiga tredjestater eller internationella organisationer att under exceptionella förhållanden skapa säkerhetsskyddsklassificerade EU-uppgifter. De nödvändiga förutsättningarna ska fastställas i informationssäkerhetsskyddsavtal. Rådets säkerhetskommitté ska få en allmän översikt innan ett informationssäkerhetsskyddsavtal ingås med en tredje part. Hierarkin mellan informationssäkerhetsskyddsavtal och administrativa överenskommelser ska förtydligas och villkoren för administrativa överenskommelser skärpas. Utvärderingsbesök ska bli obligatoriska. Säkerhetskommittén ska informeras allt effektivare om utbytet av säkerhetsskyddsklassificerade uppgifter i samband med GSFP-insatser. Ett metadataregister ska inrättas för att hantera utbytta uppgifter.

Hantering av säkerhetsrisker. Det föreslås att säkerhetsbestämmelserna kompletteras med en ny skyldighet att skydda säkerhetsskyddsklassificerade EU-uppgifter med obligatoriska säkerhetsåtgärder och att säkerhetsrisker hanteras i fråga om alla aspekter som gäller säkerhetsskyddsklassificerade EU-uppgifter. Det föreslås även att generalsekretariatet åläggs

att regelbundet utarbeta ett dokument om hotlandskap (landscape of threats) och att medlemsstaterna ska ha skyldighet att medverka till beredningen av det.

Rådets säkerhetskommitté och dess roll. Enligt rådets gällande säkerhetsbestämmelser har rådets säkerhetskommitté till uppgift att granska och bedöma alla säkerhetsfrågor inom ramen för säkerhetsbestämmelserna och i lämpliga fall lämna rekommendationer till rådet. Den ska också på uppdrag av Coreper behandla lagstiftningsförslag som rör säkerhetsbestämmelser. Rådets säkerhetskommitté och dess roll kan påverkas även av förslaget till förordning om informationssäkerhet i unionens institutioner, organ och byråer (COM(2022) 119 final), där diskussionerna om förvaltningsstrukturen har varit svåra.

3 Rättaktens rättsliga grund, subsidiaritets- och proportionalitetsprincipen

Rådets gällande säkerhetsbestämmelser har godkänts med stöd av fördraget om Europeiska unionens funktionssätt (EUF-fördraget), särskilt artikel 240.3, och rådets arbetsordning (2009/937/EU), särskilt artikel 24.

Enligt artikel 240.3 i EUF-fördraget ska rådet besluta med enkel majoritet i procedurfrågor och när det antar sin arbetsordning. Enligt artikel 24 i arbetsordningen ska rådet anta regler om säkerheten med förstärkt kvalificerad majoritet.

Enligt skäl 2 i inledningen till rådets gällande säkerhetsbestämmelser bör beslutet gälla där rådet, dess förberedande organ och rådets generalsekretariat hanterar säkerhetsskyddsklassificerade EU-uppgifter. I skäl 3 anges att i enlighet med nationella lagar och andra författningar, och i den utsträckning som krävs för rådets verksamhet, bör medlemsstaterna respektera detta beslut när deras behöriga myndigheter, personal eller entreprenörer hanterar säkerhetsskyddsklassificerade EU-uppgifter, så att de alla kan vara förvissade om att säkerhetsskyddsklassificerade EU-uppgifter ges en motsvarande skyddsnivå. I artikel 1 i de gällande säkerhetsbestämmelserna åläggs medlemsstaterna att iaktta bestämmelserna i enlighet med sina nationella lagar och andra författningar.

Rådets gällande säkerhetsbestämmelser, liksom de tidigare säkerhetsbestämmelserna, har antagits genom rådets beslut. Rådets beslut är rättsligt bindande rättsakter enligt artikel 288.4 i EUF-fördraget. Enligt artikel 4.2 i EU-fördraget hör den nationella säkerheten till medlemsstaternas befogenhet. Det är således inte möjligt att genom rådets säkerhetsbestämmelser harmonisera medlemsstaternas bestämmelser om nationell säkerhet.

I ljuset av de diskussioner som förts hittills är det sannolikt att de reviderade säkerhetsbestämmelserna antas med stöd av samma rättsliga grund som de nuvarande säkerhetsbestämmelserna. Den rättsliga grund som tillämpats tidigare kan godkännas.

I inledningen till rådets gällande säkerhetsbestämmelser anges att för att man ska kunna utveckla rådets verksamhet på alla områden som kräver hantering av säkerhetsskyddsklassificerade uppgifter bör ett övergripande säkerhetssystem för skydd av säkerhetsskyddsklassificerade uppgifter som omfattar rådet, dess generalsekretariat och medlemsstaterna inrättas. Enligt statsrådets preliminära bedömning är rådets reviderade säkerhetsbestämmelser förenliga med subsidiaritets- och proportionalitetsprinciperna.

4 Förslagets konsekvenser

Enligt en preliminär bedömning anses förslaget inte ha nämnvärda konsekvenser för Finlands myndigheter och inte heller beaktansvärda ekonomiska konsekvenser. Att rådets säkerhetsbestämmelser uppdateras leder till allt tydligare skyldigheter, ansvar och förfaranden för säkerhetsmyndigheterna och gör det lättare för myndigheterna att sköta sina uppgifter. Genom att genomföra enhetliga minimikrav för säkerheten effektivt underlättas även företagens ställning i projekt inom unionens område.

Förslagets konsekvenser ska vid behov bedömas på nytt när lagstiftningsförslagstexten blir tillgänglig i sin helhet.

5 Konsekvenser för Finlands lagstiftning

Internationell säkerhetsklassificerad information skyddas i Finland med stöd av lagen om internationella förpliktelser som gäller informationssäkerhet (588/2004). Som motivering för ”andra förpliktelser för Finland som skall iakttas av Finland” enligt 2 § 1 punkten i lagen om internationella förpliktelser som gäller informationssäkerhet anges rådets dåvarande säkerhetsbestämmelser (2001/264/EG) (RP 66/2004 rd, s 24). Enligt artikel 3 i avtalet mellan Europeiska unionens medlemsstater om skydd av säkerhetsskyddsklassificerade uppgifter som utbyts i Europeiska unionens intresse har Finland åtagit sig att vidta alla lämpliga åtgärder i enlighet med sina respektive nationella lagar och andra författningar för att iaktta rådets säkerhetsbestämmelser.

Lagen om internationella förpliktelser som gäller informationssäkerhet tillämpas på särskilt känsligt informationsmaterial. Med dessa avses sådana sekretessbelagda handlingar och material som har lämnats till finska myndigheter och som av avsändaren har markerats med en säkerhetsklass i enlighet med ett internationellt avtal eller en annan internationell förpliktelse som är bindande för Finland. När rådets nya säkerhetsbestämmelser antas tillämpas lagen om internationella förpliktelser som gäller informationssäkerhet även på de sekretessbelagda handlingar som avses i dem.

Lagen om internationella förpliktelser som gäller informationssäkerhet innehåller inte någon motsvarande klausul om skaderekvisit som lagen om offentlighet i myndigheternas verksamhet, vilket innebär att sekretessplikten för särskilt känsligt informationsmaterial inte är beroende av konsekvenserna av att informationen lämnas ut för det intresse som ska skyddas. Det informationsmaterial som skyddas enligt lagen ska sekretessbeläggas, om inte annat följer av en internationell förpliktelse som gäller informationssäkerhet (6 § 1 mom.). Sekretessplikten gäller även näringsidkare när dessa är parter i ett säkerhetsklassificerat avtal, till exempel säljare i ett upphandlingsavtal. Särskilt känsligt informationsmaterial får användas och lämnas ut endast för angivet ändamål, om inte den som bestämt materialets säkerhetsklass har samtyckt till något annat (6 § 2 mom.). När särskilt känsligt informationsmaterial produceras, kopieras, översänds, distribueras, lagras, utplånas eller hanteras i något annat avseende, skall det sörjas för att materialet skyddas på ett sätt som motsvarar säkerhetsklassen (9 § 1 mom.). I 4 § i statsrådets förordning om säkerhetsklassificering av handlingar inom statsförvaltningen (1101/2019) finns bestämmelser om säkerhetsklassificeringens motsvarighet vid tillgodoseende av internationella förpliktelser som gäller informationssäkerheten. Bestämmelsen tillämpas om inte något annat följer av internationella förpliktelser som gäller informationssäkerheten.

Enligt rådets beslut om säkerhetsbestämmelser har säkerhetsbestämmelserna inte företräde framför bestämmelserna i EU:s förordning om öppenhet 1049/2001.

Enligt 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 sådana utsedda säkerhetsmyndigheter som avses i internationella förpliktelser som gäller informationssäkerhet. De utsedda säkerhetsmyndigheterna utför de uppgifter som föreskrivs för dem i denna lag 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 Kommunikationsverket i ärenden som gäller informationssäkerhet i fråga om informationssystem och datakommunikation (4 §). Den nationella säkerhetsmyndigheten och de utsedda säkerhetsmyndigheterna kan avtala om att sköta en viss uppgift eller ett visst uppgiftsområde för den andra säkerhetsmyndighetens räkning, om ett sådant arrangemang behövs för att uppgifterna skall kunna skötas på ett ändamålsenligt, ekonomiskt och flexibelt sätt (5 §). De justeringar som föreslås i rådets säkerhetsbestämmelser ger inte upphov till ändringsbehov i de behöriga myndigheternas roller eller samarbete.

Lagen om internationella förpliktelser som gäller informationssäkerhet erbjuder fortsättningsvis ett lämpligt regelverk för skyddet av säkerhetsskyddsklassificerade EU-uppgifter i Finland. Rådets nya säkerhetsbestämmelser bedöms inte kräva ändringar i lagen, men mot bakgrunden av lagens 20 år långa tillämpningshistoria kan det vara lämpligt att i framtiden utreda om det eventuellt finns behov av att se över den.

I 4 kap. i säkerhetsutredningslagen (726/2014) finns bestämmelser om säkerhetsutredning av person och i 5 kap. om säkerhetsutredningar av företag. 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. På motsvarande sätt ska enligt 12 § en säkerhetsutredning av företag som förutsätts i en internationell förpliktelse som gäller informationssäkerhet göras på det sätt som föreskrivs i säkerhetsutredningslagen. Ett intyg över säkerhetsutredning av företag utfärdas dock av den nationella säkerhetsmyndigheten, om inte något annat följer av särskilda skäl.

6 Ålands behörighet

Regleringen av handlingars offentlighet i landskapets förvaltning och kommunalförvaltningen nämns inte uttryckligen i självstyrelselagens bestämmelser om fördelningen av lagstiftningsbehörigheten men har i huvudsak ansetts höra till landskapets behörighet. Rikets offentlighetslagstiftning kan enligt Ålands landsskapsregering tillämpas i vissa begränsade situationer vid landskapets och kommunalförvaltningens myndigheter. Enligt 60 a § i självstyrelselagen gäller rikslagstiftningen för sekretess och handlingars offentlighet i frågor som avses i 9 och 9 a kap. (förhandlingar om internationella förpliktelser och ärenden som gäller Europeiska unionen). Utöver det kan rikets offentlighetslagstiftning enligt landskapsregeringen tillämpas vid landskapets och kommunalförvaltningens myndigheter endast när de sköter uppgifter som hör till rikets behörighet.

I det fall att säkerhetsskyddsklassificerade EU-uppgifter eller handlingar överlämnas till landskapets myndigheter tillämpas enligt landskapsregeringens ståndpunkt offentlighetslagen för Åland (ÅFS 2021:79). Enligt 22 § är till en myndighet inkomna rikshandlingar eller uppgifterna i en sådan handling sekretessbelagda om handlingarna eller uppgifterna är sekretessbelagda i rikslagstiftningen. Offentlighetslagstiftningen för Åland innehåller inte olika nivåer för säkerhetsskyddsklassificerade uppgifter och inte heller bestämmelser om säkerhetsutredningar av tjänstemän.

7 Behandling av förslaget i Europeiska unionens institutioner och de övriga medlemsstaternas ståndpunkter

Rådets säkerhetsbestämmelser behandlas i den säkerhetskommitté som avses i artikel 17 i rådets beslut om säkerhetsbestämmelser som har till uppgift att granska och bedöma alla säkerhetsfrågor inom ramen för beslutet och i lämpliga fall lämna rekommendationer till rådet.

Diskussioner om en översyn av rådets säkerhetsbestämmelser inleddes i säkerhetskommittén redan 2016. I enlighet med det som beskrivs ovan i avsnittet om förslagets bakgrund har målen med diskussionerna påverkats av bland annat frågor gällande den rättsliga grunden. På grund av coronapandemin tvingades man skjuta fram revideringen av säkerhetsbestämmelserna flera gånger. Behoven av att uppdatera säkerhetsbestämmelserna har behandlats inom olika delområden och det finns inte ännu något övergripande förslag i ärendet. För närvarande uppskattas det att ett förslag om helheten kan färdigställas inom utgången av 2023, och målet är att överlämna förslaget till rådet för ett beslut så fort som möjligt efter det. Mot bakgrund av de långvariga diskussionerna kan man dra slutsatsen att medlemsstaterna kan nå samförstånd om rättsaktens detaljerade formuleringar.

8 Nationell behandling

Enligt artikel 17.2 i rådets säkerhetsbestämmelser ska rådets säkerhetskommitté bestå av företrädare för medlemsstaternas nationella säkerhetsmyndigheter. På Finlands vägnar deltog företrädare för Finlands nationella säkerhetsmyndighet i utvärderingen av rådets säkerhetsbestämmelser i säkerhetskommittén. Till den del ärendet behandlades i CIS-kommittén som är underställd säkerhetskommittén har företrädare för Transport- och kommunikationsverket deltagit i behandlingen av ärendet. I beredningen av Finlands ståndpunkter deltog förutom statsrådet även företrädare för de utsedda säkerhetsmyndigheter som avses i 5 kap. Förhandsinformation om beredningen av ärendet har getts i E-brevet E 141/2022 rd, som gällde kommissionens förslag till Europaparlamentets och rådets förordning om informationssäkerhet i unionens institutioner, organ och byråer. Denna U-skrivelse har beretts vid utrikesministeriet. I beredningen har deltagit statsrådets kansli, försvarsministeriet, Huvudstaben, Transport- och kommunikationsverket och Skyddspolisen.

U-skrivelsen har den 29 november 2023 behandlats i sektionen för hybridhot som är underställd kommittén för EU-ärenden.

9 Statsrådets ståndpunkt

Statsrådet understöder en revidering av rådets säkerhetsbestämmelser. I det reviderade beslutet beaktas på ett ändamålsenligt sätt de erfarenheter som fåtts och de översynsbehov som framkommit under de tio år som rådets gällande säkerhetsbestämmelser har tillämpats. Statsrådet understöder en omstrukturering av säkerhetsbestämmelsernas uppbyggnad så att de bestämmelser som finns i bilagorna till de nuvarande säkerhetsbestämmelserna tas in i beslutets artiklar. De nuvarande bilagorna innehåller viktig reglering, och genom att inkludera den i det egentliga beslutet blir regleringen tydligare.

I finsk lagstiftning erkänns inte tillfälliga bemyndiganden eller förlängning av PSC-intygs giltighet medan en säkerhetsutredning pågår och inte heller ad hoc-bemyndiganden i den form som föreslås nu. Statsrådet anser att det i fråga om ad hoc-bemyndigandena handlar om ett förfarande inom generalsekretariatet vid Europeiska unionens råd, där generalsekretariatet

ansvarar för den kvarstående säkerhetsrisken. Således kan förslaget godkännas även om det inte fastställs genom nationell lagstiftning.

Statsrådet anser att man i behandlingen av det parallella rättsaktsprojektet om behandling av säkerhetsskyddsklassificerade EU-uppgifter (kommissionens förslag till Europaparlamentets och rådets förordning om informationssäkerhet i unionens institutioner, organ och byråer COM(2022) 119 final) till tillämpliga delar bör beakta de lösningar som införs genom rådets nya säkerhetsbestämmelser. Enligt statsrådet är det därför motiverat att man i rådets säkerhetskommitté under innevarande år prioriterar diskussionerna om rådets reviderade säkerhetsbestämmelser.