

U 36/2021 rd

Statsrådets skrivelse till riksdagen om ett förslag till kommissionens förordningar (reglering av hanteringen av informationssäkerhetsriskerna inom luftfarten)

I enlighet med 96 § 2 mom. i grundlagen översänds till riksdagen Europeiska unionens byrå för luftfartssäkerhets förslag av den 11 juni 2021 till kommissionens förordningar om reglering av hanteringen av informationssäkerhetsriskerna inom luftfarten samt en promemoria om förslaget.

Helsingfors den 15 juli 2021

Kommunikationsminister Timo Harakka

Överinspektör Sonja Töyrylä

KOMMUNIKATIONSMINISTERIET PROMEMORIA

15.7.2021

FÖRSLAG TILL KOMMISSIONENS FÖRORDNINGAR (REGLERING AV HANTERINGEN AV INFORMATIONSSÄKERHETSRISKERNA INOM LUFTFARTEN)

1 Bakgrund

Europeiska unionens byrå för luftfartssäkerhet (EASA) lämnade den 11 juni 2021 till EU-kommissionen sitt förslag till reglering av informationssäkerheten inom luftfarten (*EASA Opinion No 03/2021*). EASA:s författningsförslag finns tillgängliga på adressen: <https://www.easa.europa.eu/document-library/opinions/opinion-032021>. Som bilaga till förslaget lämnade EASA utkast till kommissionens genomförandeförordningar och delegerade förordningar som underlag för kommissionens beredning. Kommissionens behörighet att utfärda förordningar grundar sig på den nya så kallade EASA-förordningen som trädde i kraft den 11 september 2018 (Europaparlamentets och rådets förordning (EU) 2018/1139 om fastställande av gemensamma bestämmelser på det civila luftfartsområdet och inrättande av Europeiska unionens byrå för luftfartssäkerhet, och om ändring av Europaparlamentets och rådets förordningar (EG) nr 2111/2005, (EG) nr 1008/2008, (EU) nr 996/2010, (EU) nr 376/2014 och direktiv 2014/30/EU och 2014/53/EU, samt om upphävande av Europaparlamentets och rådets förordningar (EG) nr 552/2004 och (EG) nr 216/2008 och rådets förordning (EEG) nr 3922/91). Riksdagen informerades om beredningen av EASA-förordningen med en U-skrivelse den 11 februari 2016 (U 6/2016 rd).

Med de föreslagna förordningarna eftersträvas en mer heltäckande och övergripande reglering av informationssäkerheten inom luftfartens område. För närvarande är lagstiftningen om informationssäkerheten inom uttryckligen luftfarten antagen genom kommissionens genomförandeförordning (EU) 2015/1998 som antagits med stöd av den så kallade förordningen om skyddet för den civila luftfarten (Europaparlamentets och rådets förordning (EG) nr 300/2008 om gemensamma skyddsregler för den civila luftfarten och om upphävande av förordning (EG) nr 2320/2002). Den gällande lagstiftningen täcker hanteringen av informationssäkerhetsrisker avseende säkerhetsåtgärderna (*aviation security*) inom luftfarten och gäller i praktiken närmast organisationer verksamma på flygfält, men kommissionens nu föreslagna förordningar skulle beakta informationssäkerhetsriskernas konsekvenser även för en säker luftfart (*aviation safety*).

Dessutom är den föreslagna regleringen mer täckande och övergripande än regleringen i EU:s direktiv om nät- och informationssäkerhet, det vill säga NIS-direktivet (Europaparlamentets och rådets direktiv (EU) 2016/1148 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen). NIS-direktivet tillämpas endast på centrala servicetillhandahållare angivna av medlemsstaterna, medan kommissionens föreslagna förordningar skulle täcka nästan alla viktiga aktörsgrupper inom luftfartssystemet.

2 Förslagens syfte

Förslagens syfte är att effektivisera luftfartssektorns möjligheter att skydda sig mot informationssäkerhetsrisker samt att förbättra flygsäkerheten. Säkerhetsregleringen inom luftfarten har traditionellt syftat till att minska sannolikheten för olyckor och allvarliga följder, men med de nu föreslagna förordningarna vill man fästa uppmärksamhet även vid medvetet utnyttjande av befintliga svagheter i informationssäkerheten. Luftfartssektorns informationssystem står i allt

högre grad i kontakt med varandra och även risken för avsiktligt missbruk av svagheter i systemet har ökat. Dessutom förebygger säkra informationssystem situationer då fel data eller en felaktig funktion oavsiktligt kommer in i systemet och påverkar den operativa säkerheten.

Det är värt att beakta att inom luftfarten skyddar informationssäkerhetsregleringen utöver personuppgifter och integritet även betydande allmänna och enskilda intressen. Informationssäkerhetsriskerna kan leda till situationer som har direkt koppling till flygets säkerhet samt människors liv och hälsa. Störningar i systemet påverkar även direkt luftfartssystemets funktion, till exempel genom att lamslå flygfältets verksamhet eller flygtrafiken.

Lagstiftningens huvudsakliga syfte är att säkerställa att de organisationer och myndigheter som medverkar i den civila luftfartens verksamhet kan identifiera, skydda sig mot, upptäcka, reagera på och återhämta sig från informationssäkerhetshändelser som påverkar flygsäkerheten.

3 Förslagets huvudsakliga innehåll

Till följd av den civila luftfartens internationella karaktär är regleringen av sektorn mycket internationellt inriktad och EU-inriktad. Även regleringen av luftfartssäkerheten, både när det gäller flygsäkerheten och skyddsåtgärderna inom den civila luftfarten, har till stor del harmoniserats inom EU med direkt tillämpliga förordningar. Den föreslagna informationssäkerhetsregleringen skulle utfärdas med stöd av EASA-förordningen om luftfartens säkerhet. Med EASA-förordningen har kommissionen getts befogenhet att föreskriva om mer detaljerade krav genom flera olika genomförandeförordningar och delegerade förordningar. I EASA-förordningen ställs också olika krav på utfärdandet av bestämmelser på lägre nivå beroende på vilka aktörer bestämmelserna gäller.

I förslaget ställs krav dels på organisationernas och myndigheternas hantering av informationssäkerheten, dels på myndigheterna gällande certifiering och tillsyn. På grund av systematiken i EASA-förordningen har den nya föreslagna regleringen behövt indelas i kommissionens genomförandeförordning och delegerade förordning. I förslaget ingår sammanlagt fyra utkast till förordningar av kommissionen. Av dessa innehåller två ny reglering, dvs. de ställer krav på hanteringen av informationssäkerhetsrisker, informationssäkerhetshändelser och personuppgiftsincidenter. Förordningarna är innehållsligt nästan identiska, men den delegerade förordningen tillämpas på konstruktions- och tillverkningsorganisationer, flygplatsoperatörer och leverantörer av ledningstjänster för trafik på plattan, medan genomförandeförordningen tillämpas på alla andra aktörer. Med de två andra kommissionens förordningar föreslås däremot att kommissionens gällande förordningar (EU) nr 748/2012, nr 1321/2014, 2017/373, 2015/340, nr 139/2014, nr 1178/2011, nr 965/2012 och 2021/664 ändras så att det till dem fogas behövliga bestämmelser om myndigheternas certifierings- och tillsynsuppgifter.

Behovet att harmonisera den föreslagna regleringen med NIS-direktivet som bereds som bäst har identifierats i förordningsförslagen. I dem beaktas eventuella överlappningar och luckor på så sätt att de nationella myndigheterna ska samordna kraven i den föreslagna regleringen med avseende på åtgärderna som krävs enligt NIS-direktivet och annan överlappande EU-lagstiftning. Dessutom kan den behöriga myndigheten ersätta kraven i den föreslagna regleringen med kraven i NIS-direktivet eller annan EU-lagstiftning eller nationell lagstiftning om dessa motsvarar minst kraven i den föreslagna regleringen. Finland har för närvarande ingen reglering av den föreslagna omfattningen.

Enligt förslaget ska lagstiftningen tillämpas på en bred skara aktörer inom luftfarten: behöriga myndigheter, konstruktions-, tillverknings- och underhållsorganisationer, flygbolag, luftvärdig-

hetsorganisationer, flygmedicinska center, operatörer av flygsimulerande utbildningshjälpmedel (FSTD), tillhandahållare av flygtrafik- eller flygkontrolltjänster, tillhandahållare av flygtrafiktjänster för obemannad luftfart, dvs. tillhandahållare av U-space-tjänster, tillhandahållare av gemensamma informationstjänster för U-space-lufterum, flygplatsoperatörer. Dessutom föreslås att lagstiftningen ska tillämpas på andra än organisationer som bedriver endast teoretisk utbildningsverksamhet.

Utanför lagstiftningens tillämpningsområde hamnar för det första aktörer inom lätt luftfart, dvs. ELA2-verksamhet (ELA2-verksamhet definieras i kommissionens förordning (EU) nr 748/2012 artikel 1.j). I praktiken gäller den till exempel luftballonger och luftfartyg under 2 000 kg.

Lagstiftningen ska inte heller tillämpas på kategorierna ”öppen” eller ”specifik” för obemannade luftfartyg annat än i vissa fall. I EU-regleringen och den nationella reglering som grundar sig på den indelas verksamhet med obemannade luftfartyg enligt risk i tre kategorier: öppen, specifik och certifierad. I kategorierna öppen och specifik handlar det om verksamhet med låg eller förhöjd risk. Merparten av den obemannade luftfarten i dag hör till lågriskkategorierna. För verksamhet med hög risk, dvs. kategorin ”certifierad” är avsikten att beslutet om tillämpningen av den föreslagna regleringen fattas senare och separat i en annan lagstiftningsprocess. Verksamheten i kategorin certifierad påminner om bemannad luftfart, dvs. transport av människor och gods. I praktiken bedrivs ännu inte verksamhet i högriskkategorierna i Finland.

På samma sätt är avsikten att beslutet om tillämpningen gällande tillhandahållare av marktjänster fattas senare separat i samband med den lagstiftningsprocess där mer exakta säkerhetskrav för marktjänsterna på EU-nivå utvecklas. Marktjänsterna inkluderades i EASA-regleringens tillämpningsområde i samband med den senaste revideringen av EASA-förordningen och samtidigt håller man för första gången på att utveckla gemensamma exaktare säkerhetskrav på EU-nivå för dem. Med marktjänster avses tjänster som flygbolagen behöver som stöd för trafikeringen. Sådana tjänster är till exempel bränslepåfyllnings-, lastbeskeds- och frakttjänster. Marktjänsterna omfattar även flygklarerings-, catering-, bagagehanterings- och transporttjänster på flygfälten.

Utanför tillämpningsområdet faller även sådana aktörer i ett tredjeland på vilka kommissionens förordning (EU) nr 452/2014 (Kommissionens förordning nr 452/2014 om tekniska krav och administrativa förfaranden avseende flygdrift som utförs av operatörer från tredjeland i enlighet med Europaparlamentets och rådets förordning (EG) nr 216/2008) eller bilaterala säkerhetsavtal tillämpas. Regleringen tillämpas inte heller på en sådan organisation som visar den behöriga myndigheten att dess verksamhet inte utgör en sådan informationssäkerhetsrisk som påverkar dess egen eller någon annan organisations säkerhet eller på vilken EASA-förordningen inte tillämpas. Regleringen lämpar sig inte heller för sådana organisationer för vilkas verksamhet det inte ställs krav i den gällande regleringen. Sålunda tillämpas inte de föreslagna förordningarna till exempel på underleverantörer till aktörer som omfattas av regleringen, utan det är på de aktörernas ansvar att beakta informationssäkerhetsriskerna i sina avtalspartners verksamhet och se till att riskhanteringen är beaktad i avtalet mellan parterna.

Regleringens centrala princip är risk- och prestationsbaserad. Med regleringen åläggs organisationer och myndigheter skyldigheter att hantera informationssäkerhetsriskerna inom luftfarten och krav på prestationsförmåga för att uppfylla målen. Regleringen tar inte ställning till vilka metoder som används och ställer inte heller mer detaljerade krav på det praktiska utförandet. I kraven på olika organisationer är avsikten alltså att beakta verksamhetens art och de därmed förknippade informationssäkerhets- och flygsäkerhetsriskerna. Utgångspunkten för den reviderade EASA-förordningen var också en risk- och prestationsbaserad ansats. I praktiken innebär regleringen för aktörerna att de bör identifiera informationssäkerhetsriskerna i sin verksamhet

och ta fram en plan för att hantera dem. Dessutom förutsätts att aktörerna vidtar åtgärder för att begränsa konsekvenserna av informationssäkerhetshändelser och för att återhämta sig från dem.

EASA bereder som bäst mer detaljerat material avsett till stöd för genomförandet av den föreslagna regleringen. EASA har för avsikt att komma med godtagbara sätt att uppfylla kraven som komplement till förordningarna (*acceptable means of compliance*) och material för vägledning (*guidance material*) efter att kommissionen har antagit de slutliga förordningarna.

De föreslagna förordningarna avses börja tillämpas ett år efter att de trätt i kraft. Organisationerna har dock möjlighet att åtgärda missförhållanden som myndigheterna påpekar under två år efter att förordningarna har trätt i kraft. Den nationella myndigheten (i Finland Transport- och kommunikationsverket) kan dock besluta även om en längre tidsfrist.

4 Förslagets rättsliga grund

Enligt artikel 290.1 i fördraget om Europeiska unionens funktionssätt (FEUF) kan det i en lagstiftningsakt till kommissionen delegeras befogenhet att anta akter med allmän räckvidd som inte är lagstiftningsakter och som kompletterar eller ändrar vissa icke väsentliga delar av lagstiftningsakten (delegerade rättsakter). Dessutom gäller enligt artikel 291.2 i FEUF att om enhetliga villkor för genomförande av unionens rättsligt bindande akter krävs, ska kommissionen tilldelas genomförandebefogenheter genom dessa akter (genomförandeakter).

Kommissionens behörighet att anta de nu föreslagna förordningarna baserar sig på Europaparlamentets och rådets förordning (EU) 2018/1139 om fastställande av gemensamma bestämmelser på det civila luftfartsområdet och inrättande av Europeiska unionens byrå för luftfartssäkerhet, det vill säga den så kallade EASA-förordningen som antagits i normal lagstiftningsordning.

Den delegerade lagstiftningsmakten grundar sig på artikel 19.1 och artikel 39.1 i EASA-förordningen.

Behörigheten att anta genomförandeakter baserar sig på artikel 17.1, artikel 27.1, artikel 31.1, artikel 43.1, artikel 53.1 och artikel 62.15 c i EASA-förordningen. Genomförandeförordningarna antas i enlighet med artikel 127 i EASA-förordningen enligt det kommittégranskningsförfarande som avses i artikel 5 i Europaparlamentets och rådets förordning (EU) nr 182/2011.

Statsrådet anser att förslagen är överensstämmande med deras rättsliga grund.

5 Förslagets konsekvenser

Konsekvenser för myndigheternas verksamhet

I Finland är Transport- och kommunikationsverket nationell myndighet för den civila luftfarten. Regleringen bedöms påverka myndighetens verksamhet eftersom antalet aktörer som omfattas av tillsyn kommer att öka avsevärt jämfört med aktörerna enligt NIS-direktivet. I förordningarna föreslås att regleringen ska övervakas av samma myndighet som övervakar ifrågavarande organisationers verksamhet även till övriga delar. Medlemsstaterna kan emellertid om de så vill utse även en annan myndighet till behörig myndighet. I Finland skulle Transport- och kommunikationsverket vara en given myndighet för detta. Det större antalet aktörer som ingår i tillsynen bedöms öka Transport- och kommunikationsverkets uppgifter och på det sättet påverka myndigheternas verksamhet. Konsekvenserna för myndigheternas ekonomiska behov och behov av personresurser kan bedömas närmare först när behandlingen av den föreslagna regleringen går

vidare och det kompletterande materialet blir klart. Konsekvenserna för myndighetsverksamheten beror på hur tillsynen ordnas i praktiken, men i den fortsatta beredningen är strävan att lindra den ytterligare administrativa börda som förslaget ger upphov till. Resursmässiga och eventuella andra konsekvenser till följd av förslaget bör bedömas mer ingående när förslaget behandlas och besluten om den nationella resurstilldelningen fattas på normalt sätt i förfarandena i anslutning till budgeten och planen för de offentliga finanserna.

Konsekvenser för den nationella lagstiftningen

Den föreslagna regleringen utgörs av direkt tillämpliga förordningar och kräver därför inte genomförandeåtgärder. Bestämmelser om den nationella luftfarten finns i luftfartslagen (864/2014) och lagen om transportservice (320/2017). I 128 a § i luftfartslagen föreskrivs om skyldigheten att sörja för riskhanteringen i fråga om kommunikationsnät och informationssystem och i 128 b § om rapportering av informationssäkerhetshändelser. Med dessa paragrafer har kraven gällande luftfarten i NIS-direktivet genomförts nationellt. Den gällande lagstiftningen om luftfart bör sannolikt ändras för att beakta den direkt tillämpliga EU-regleringen och undvikandet av överlappningar.

Ekonomiska konsekvenser för aktörer inom luftfart

Den föreslagna regleringens konsekvenser för luftfartsaktörerna beror i hög grad på hurdana informationssäkerhetssystem och rutiner de har samt vilka informations- och flygsäkerhetsrisker verksamheten är förknippad med. Luftfartssektorn är strikt reglerad och redan nu ställs det avsevärda krav på olika aktörer och deras system för säkerhetshantering. Dessutom handlar det i huvudsak om stora aktörer som bedöms ha god beredskap att uppfylla kraven i regleringen. Samtidigt kan realiserade informationssäkerhetsrisker i form av allvarliga informationssäkerhetshändelser eller händelser med inverkan på flygsäkerheten orsaka stora kostnader för både en enskild luftfartsorganisation och luftfarten mer omfattande. På lång sikt kan man anta att de ekonomiska konsekvenserna är positiva. Dessutom ger ett informationssäkert möjliggörande av digitaliseringen både ekonomiska och miljömässiga fördelar.

6 Förslagets förhållande till grundlagen samt de grundläggande och mänskliga rättigheterna

Regleringen bedöms inte ha några betydande konsekvenser i förhållande till grundlagen eller de grundläggande och mänskliga rättigheterna. Den skulle dock ha positiva konsekvenser framför allt för individernas säkerhet och den personliga integriteten. Regleringen syftar till att förebygga händelser som påverkar människors liv och hälsa. Dessutom påverkar regleringen skyddet för privatlivet på ett positivt sätt, eftersom utvecklingen av informationssäkerhetssystemen även förbättrar skyddet av personuppgifter.

7 Ålands behörighet

Enligt 27 § 14 punkten i självstyrelselagen för Åland (1144/1991) har riket lagstiftningsbehörighet i fråga om luftfart. Förordningsförslagen hör således till rikets lagstiftningsbehörighet.

8 Behandlingen av förslaget i Europeiska unionens institutioner och de övriga medlemsstaternas ståndpunkter

EASA:s förslag har utarbetats av EASA. Beredningen har fått stöd av en expertgrupp där en representant för Transport- och kommunikationsverket ingår. I beredningen har även intressentgrupper hörts. EASA:s författningsutkast har varit på för alla öppen remiss 27.5–27.9.2019. Intressentgrupperna har kunnat lämna sina kommentarer till utkastet direkt till EASA.

EASA:s förordningsförslag har getts som grund för kommissionens beredning. Förordningsförslagen behandlades första gången vid EASA-kommitténs möte 22.6–23.6.2021 och behandlingen fortgår under 2021. Det mer exakta tidsschemat, som när omröstningen om förordningarna görs, är ännu inte känt. Omröstningen antas ske 2022.

Expertberedning på EU-nivå har pågått under flera år. Under beredningen har inga betydande inkonsekvenser framkommit.

9 Nationell behandling av förslaget

Utkastet till en U-skrivelse om regleringsförslaget behandlades i transportsektionens (EU 22) skriftliga förfarande 22.6.2021–24.6.2021. Dessutom begärdes kommentarer av kommunikationsministeriets nätverk av intressentgrupper inom flygtrafiken. Det kom in två kommentarer, som har beaktats i U-skrivelsen. I statsrådets ståndpunkt och i konsekvenserna för myndigheternas verksamhet tillfogades ett omnämnande av att strävan i den fortsatta behandlingen är att lindra den ytterliga administrativa börda som förslaget ger upphov till. Dessutom lades det i statsrådets ståndpunkt till ett omnämnande om sammanjämkning av regleringen utöver med direktivet om nät- och informationssäkerhet även med regleringen av säkerhetsåtgärderna inom luftfarten.

10 Statsrådets ståndpunkt

Statsrådet understöder förslagets mål att förbättra cybersäkerheten inom luftfartssektorn. Den föreslagna regleringen skulle förbättra luftfartssäkerheten genom systematisering och standardisering av luftfartsaktörernas informationssäkerhetspraxis. Statsrådet anser det vara viktigt att regleringen av luftfartssäkerheten utvecklas så att den motsvarar de behov och nya säkerhetshot som identifierats i sektorn.

Den föreslagna regleringen tillämpas på en stor skara aktörer, vilket kan anses vara en bra utgångspunkt för att trygga att regleringen får en tillräcklig täckning. Statsrådet anser även att de föreslagna begränsningarna av tillämpningsområdet är lämpliga. Att tillämpa regleringen till exempel på den lätta luftfarten eller obemannade luftfartyg med låg eller förhöjd risk har i detta skede inte bedömts vara ändamålsenligt på grund av verksamhetens annorlunda karaktär. Statsrådet understöder även att tillämpningen av regleringen på marktjänsterna och obemannad luftfart med hög risk utreds separat. För dessa funktioner bereds noggrannare säkerhetsbestämmelser först nu, varför det vore bra att utreda även kraven på hanteringen av informationssäkerhetsriskerna som en del av dessa helheter och förvaltningssystemkrav med beaktande av sektorns praxis.

Statsrådet understöder även risk- och prestationsprincipen som förordningsförslagen utgår från. Eftersom regleringens tillämpningsområde är brett, är det viktigt att man når nivån på de förutsatta åtgärderna anges kan beakta aktörernas storlek och verksamhetens inverkan på luftfartssäkerheten. Dessutom anser statsrådet det vara viktigt att aktörerna ges tillräckligt med tid för anpassning till den förändrade regleringen.

Statsrådet anser det vara viktigt att man vid granskningen av de ytterligare uppgifter som föreslås för tillsynsmyndigheterna försöker lindra den ytterligare administrativa börda som förslaget

ger upphov till. Besluten om den nationella resurstilldelningen fattas på normalt sätt i förfarandena för budgeten och planen för de offentliga finanserna.

Statsrådet anser det vara viktigt att den föreslagna regleringen sammanjämkas med den övriga EU-lagstiftningen. Särskild vikt bör fästas vid den ändring av direktivet om nät- och informationssäkerhet som bereds och regleringen av säkerhetsåtgärderna inom luftfarten. Det är viktigt att regleringen bildar en samlad helhet där medlemsstaterna eller aktörerna inom luftfarten inte åläggs överlappande eller motstridiga skyldigheter.