Luftfartstilsynet
CIVIL AVIATION AUTHORITY - NORWAY

Notat

Dato
13.12.2019

Referanse
19/12808-4

Saksbehandler
Sissel W. Strandås, tlf. +47 99778755

Til
Alminnelig høringsliste

Kopi til

Høring - Endring til forordning (EU) 2015/1998 – tiltak for en bedre og robust cybersecurity

1. Høring

Luftfartstilsynet foreslår på vegne av Samferdselsdepartementet å gjøre endring i forskrift 1. mars 2011 nr. 214 om forebyggelse av anslag mot sikkerheten i luftfarten mv. (securityforskriften). Forskriften gjennomfører kommisjonsforordning (EU) 2015/1998 som fastsetter de detaljerte tiltakene for gjennomføring av felles grunnleggende standarder for luftfartssikkerhet.

Med jevne mellomrom er det behov for endring og klargjøring av securityregelverket. Det ble vedtatt endringer i forordning (EU) 2015/1998 ved votering i AVSEC-møtet som fant sted juni 2019. Den vedtatte rettsakten ble publisert i Official Journal 25. september 2019. De nye kravene i regelverket trer i kraft 31. desember 2020.

Endringene som omtales i høringen her omfatter i det vesentligste nye krav til tiltak for å håndtere og tilrettelegge for en robust cybersecurity. De nye reglene stiller krav både til myndighetene og til relevante luftfartsaktører som omfattes av forordning (EU) 300/2008. Vedtatt endringsforordning (EU) 2019/1583 ligger vedlagt høringen her.

Svar på høringen må være Luftfartstilsynet i hende 15. februar 2020. Høringssvar bes sendt på epost til postmottak@caa.no. Alternativt kan høringssvar sendes per post til Luftfartstilsynet, Postboks 243, 8001 Bodø. Det bes om at svar merkes med saksnummer: 19/12808.

2. Bakgrunn – hovedinnhold i regelverket

Endringsforordningen stiller krav til at myndigheter, flyplassoperatører, luftfartsselskaper og andre berørte enheter foretar effektive sikkerhetsrisikovurderinger knyttet til deres virksomhet for å styre og håndtere cybersecurityrisiko relatert til systemer brukt i sivil luftfart. Berørte myndigheter og enheter må også ha tiltak og planer for å håndtere trusler til cybersecurity.

Lufthavnoperatører, luftfartsselskaper og enheter som er definert i nasjonalt sikkerhetsprogram for sivil luftfart må identifisere og beskytte deres kritiske informasjons- og kommunikasjonsteknologi og data fra cybersecurityangrep som kan påvirke sikkerheten i sivil luftfart. Lufthavnoperatører, luftfartsselskaper og enheter skal i sine sikkerhetsprogram eller relevant dokument som er kryssreferert i sikkerhetsprogrammet identifisere kritisk informasjons- og

kommunikasjonsteknologisystemer og data. Samtidig skal de spesifisere tiltakene for å sikre beskyttelse mot, deteksjon av, respons på og gjenoppretting fra cyberangrep som kan påvirke sikkerheten til sivil luftfart.

De detaljerte tiltakene skal beskytte systemer og data fra ulovlig inngrep. Tiltakene skal identifisere trusler mot cybersecurity og være utviklet og implementert i samsvar med en risikovurdering utført av lufthavnoperatøren, luftfartsselskapet eller enheten.

Ett av formålene med endringsforordningen er å sikre samsvar med andre cybersecurityregelverk som er relevant for luftfart. Med innføringen av NIS-direktivet og det kommende cybersecurityregelverket fra EASA er det ventet at det ikke vil forekomme regelverkshull eller dobbeltregulering med annet relevant cybersecurityregelverk.

Dersom lufthavnoperatører, luftfartsselskaper, og enheter som definert i nasjonalt sikkerhetsprogram for sivil luftfart er underlagt særskilte krav til sikkerhet for cybersecurity som følger av annen EU-lovgivning eller nasjonal lovgivning, skal aktuell myndighet samordne med andre relevante kompetente myndigheter for å sikre samordnede eller kompatible overvåkingsregimer.

I tillegg stilles det nye krav til personellgrupper som skal underlegges bakgrunnssjekk. Fra 31. desember 2020, skal følgende personell ha bestått kravene til enten utvidet eller standard bakgrunnssjekk:

a) *Persons being recruited to implement, or to be responsible for the implementation of, screening, access control or other security controls elsewhere than a security restricted area*
b) *Persons having unescorted access to air cargo and mail, air carrier mail and air carrier material, in-flight supplies and airport supplies to which the required security controls have been applied.*
c) *Persons having administrator rights or unsupervised and unlimited access to critical information and communications technology systems and data used for civil aviation security purposes as described in 1.7.1 in accordance with the national security programme, or having been otherwise identified in the risk assessment in accordance with 1.7.3.*

Med mindre annet er angitt i forordningen skal det fastsettes nasjonalt av egnet myndighet (Luftfartstilsynet) i henhold til gjeldende nasjonale regler om en utvidet eller standard bakgrunnssjekk skal fullføres for de nevnte personellgrupper. Luftfartstilsynet ber særskilt om innspill fra mottakerne vedrørende dette.

Når det gjelder opplæring og rekruttering, skal personer som er ansvarlig for detaljerte tiltak som skal beskytte systemer og data fra ulovlig inngrep ha tilstrekkelige ferdigheter og kvalifikasjoner som kreves for å kunne utføre sine utpekte oppgaver effektivt. De skal gjøres oppmerksom på relevante risikoer mot cybersecurity basert på "need to know". Videre skal personer som har tilgang til data eller systemer få passende og spesifikk jobbrelatert opplæring i samsvar med deres rolle og ansvar, herunder bli gjort kjent med relevante risikoer der deres stillingsfunksjon krever dette. Det er i skrivende stund ikke blitt publisert veiledningsmateriale fra EU-Kommisjonen som definerer hva opplæringen skal inneholde.

3. Luftfartstilsynets vurdering

Dette høringsnotatet er utarbeidet i tråd med de føringer som ligger i regjeringens utredningsinstruks. Et minimumskrav er da å besvare følgende spørsmål:

- Hva er problemet, og hva vil vi oppnå?
- Hvilke tiltak er relevante?
- Hvilke prinsipielle spørsmål reiser tiltakene?
- Hva er de positive og negative virkningene av tiltakene, hvor varige er de, og hvem blir berørt?
- Hvilket tiltak anbefales, og hvorfor?
- Hva er forutsetningene for en vellykket gjennomføring?

3.1 Hva er problemet, og hva vil vi oppnå?

Det er et økende fokus på håndteringen av trusselen mot cybersecurity. Endringsforordningen til forordning (EU) 2015/1998 skal bistå medlemslandene i å sikre full overensstemmelse med endringer i ICAO Annex 17 og nylig innførte standarder og anbefalinger som var gjeldende i henhold til ICAO Annex 17 fra 16. november 2019.

EASA forbereder nytt regelverk for cybersecurity i luftfart. Kravene som foreslås vil gjelde for alle organisasjoner som har en EASA-godkjenning og organisasjoner som for tiden har krav til styringssystemer i eksisterende EASA-regelverk. Noen av disse organisasjonene kan også falle innenfor virkeområdet til forordning (EU) 300/2008 (for eksempel kommersielle luftfartsselskaper). Ny endringsforordning til forordning (EU) 2015/1998 er utformet slik at dersom disse organisasjonene følger kravene i det kommende EASA-regelverket om cybersecurity, vil de også oppfylle kravene i endringsforordningen (EU) 2019/1583. Og vice versa.

I tillegg kan det være organisasjoner som omfattes av virkeområdet for NIS-direktivet fordi de har blitt definert som tilbydere av samfunnsviktige tjenester. Følger disse organisasjonene de kravene som gjelder av NIS-direktivet, vil de også ha oppfylt kravene etter endringsforordning (EU) 2019/1583.

Det betyr at de organisasjonene som ikke omfattes av EASA-regelverket eller NIS-direktivet, men som faller innenfor området til forordning (EU) 300/2008, må overholde kravene som følger av de nye cybersecurityreglene i endringsforordning (EU) 2019/1583 som endrer forordning (EU) 2015/1998.

Felles formål for regelverkene er å sikre en robust cybersecurity samt sørge for at både myndigheter og organisasjoner iverksetter detaljerte tiltak, planer og prosedyrer for å håndtere trusselen mot cybersecurity og minimere/redusere omfanget dersom et cybersecurityangrep finner sted.

3.2 Hvilke tiltak er relevante

Endringsforordningen endrer en forordning som allerede er tatt inn i EØS-avtalen og gjennomført i norsk rett gjennom forskrift 1. mars 2011 nr. 214 om forebyggelse av anslag mot sikkerheten i luftfarten mv. (securityforskriften) § 3. Endringsforordningen må følgelig gjennomføres gjennom endring av forskriften.

Ingen andre tiltak er relevante.

3.3 Hvilke prinsipielle spørsmål reiser tiltakene?

Saken reiser ingen prinsipielle spørsmål slik dette er angitt i utredningsinstruksen.

3.4 Hva er de positive og negative virkningene av tiltakene, hvor varige er de, og hvem blir berørt?

Det er et økende fokus på håndtering av trusselen mot cybersecurity. De positive sidene av tiltaket er at myndigheter og organisasjoner må forbedre sine sikkerhetsprogram, planer og prosedyrer for å sikre en mer robust cybersecurity og være bedre rustet mot og kunne hindre eventuelle cybersecurityangrep. Nye krav til bakgrunnssjekk og opplæring for alt personell med ansvar for IT-sikkerhet, sikrer sivil luftfart mot utro tjenere som rammer sivil luftfart gjennom angrep mot elektroniske styringssystemer og data. Det forutsettes at de nye kravene skal øke bevisstheten vedrørende trusselen mot cybersecurity. Dette vil formodentlig tale for en forbedret security innen sivil luftfart.

Luftfartstilsynet har ikke identifisert negative virkninger av tiltaket.

Tiltaket berører luftfartsmyndigheten, flyplassoperatører, luftfartsselskaper og andre enheter som er omfattet av forordning (EU) 300/2008. Virkningene av tiltakene er varige.

3.5 Hvilket tiltak anbefales, og hvorfor?

Forslaget til endringsforordning endrer som nevnt forordning (EU) nr. 2015/1998 som allerede er tatt inn i EØS-avtalen og gjennomført i norsk rett gjennom forskrift 1. mars 2011 nr. 214 om forebyggelse av anslag mot sikkerheten i luftfarten mv. (securityforskriften).

Rettsaktene må besluttes innlemmet i EØS-avtalen før de kan tas inn i norsk rett. Rettsaktene vil være gjeldende i EU 31.12.2020. Gjennomføring i norsk rett vil bli gjort ved at rettsakten gjennomføres i forskrift 1. mars 2011 nr. 214 om forebyggelse av anslag mot sikkerheten i luftfarten mv. § 3. Se for øvrig vedlagte utkast til endringsforskrift. Rettsakten medfører ikke ytterligere endringer i securityforskriften.

3.6 Hva er forutsetningene for en vellykket gjennomføring?

En vellykket gjennomføring forutsetter at de norske aktørene tilpasser sine prosedyrer til de nye reglene.