



FORENINGEN AF RÅDGIVENDE INGENIØRERS HØRINGSSVAR

Kommissionens handlingsplan for dronesikkerhed og anti-dronesikkerhed.

Til: **Transportministeriet**

Att: Marie Hedensted Lundorf, Sofie Albrechtsen, Marius Keller, Liv Frank, Karoline Jakobsen, Lasse Kristoffersen, Henriette Pia Meldgaard Kristensen, og Maya Nielsen

Fra: **Foreningen af Rådgivende Ingeniører (FRI)**

Konsekvenser for erhvervsbrug af droner i EU efter Action Plan on Drone & Counter-Drone Security (2026)

Tak for muligheden for at kommentere på EU's nye handlingsplan, der skal skærpe sikkerhed og ansvarlighed i droneøkosystemet. Forslaget har stor betydning for FRI, da en stor del af vores medlemmer – ligesom resten af byggebranchen – benytter de helt små droner i deres daglige arbejde. Formålet om at skærpe sikkerheden er forbilledligt, men droner mellem 100 og 250 g. er af en størrelse, der ikke bør vurderes at have en sikkerhedsrisiko. Det bør derfor tilstræbes, at de helt små droner kan anvendes uden yderligere bureaukrati og frem for alt, at de ikke kommer over 250 g., idet dette medfører et krav om, at droneføreren skal have dronecertifikat.

Opsummering:

Registrering af droner over 100 g.

Det er FRI's vurdering, at kravet vil fordyre det at eje droner, hvilket går ud over brancher, som benytter droner i deres virksomheder fx inden for byggeri.

FRI anbefaler at begrænse kravet til at tilknytte drone-ID én gang til operatør-ID. Denne løsning vil være betydeligt mere overkommelig for branchens virksomheder.

Fjern-ID

FRI frygter, at krav til Remote-ID vil tilføje ekstra "payload" til de lette droner, da det kan bringe vægten over 250g, hvilket medfører krav om dronecertifikat, samt forbud mod at overflyve uvedkommende mennesker.



Take-off kræver gyldig operatør ID

Droner uden godkendt ID vil i praksis ikke kunne tages i brug, og FRI frygter, at den daglige anvendelse af dronen kan blive ødelagt ved nedetid eller fejl i registrene, så med kravet følger en forpligtelse til et fejlfrit teknisk system.

Geofencing

FRI vurderer, at manglende overholdelse kan begrænse adgangen til erhvervsopgaver, samt at kravet indebærer en risiko for, at geofencing kan blive så omfattende, at det vil begrænse fordelene ved droneanvendelse i branchen.

FRI foreslår derfor, at geofencing følges op af en mulighed for hurtigere og lempeligere dispensationsadgang. Det vil fx være af afgørende betydning for branchen, at en byggeplads med +50m i omkreds fritages fra geofencing, hvis branchen skal kunne bruge droner effektivt.

U-space

FRI frygter, at U-space kan være særligt omkostningsfuldt for mindre droneaktører, der skal holde software og systemer ajour. En undtagelse fra U-space for droner under 250g vil være hensigtsmæssig, da disse er særdeles skrøbelige over for hardwarekrav - for skubbes droner op i vægt over 250g, vil krav om dronecertificat være en betydeligt fordyrende faktor i anvendelsen af droner.

Uddybende bemærkninger til de enkelte forslag:

Skærpede krav til registrering og identifikation

Krav om registrering af flere droner (Ref.: s. 6, 9–10)

Planen indfører obligatorisk registrering af alle droner over 100 gram. Registreringen knytter dronen til dens operatør for at sikre entydigt ansvar. Virksomheder får dermed pligt til at administrere deres registreringer.

Det er FRI's vurdering, at dette medfører et ekstra lag af bureaukrati, som vil fordyre det at eje droner, og dermed ligge hindringer i vejen for brancher, som har stor gavn af droner. I stedet foreslår FRI, at det bør være en 1-gangsopgave at tilknytte drone-ID til operatør-ID, hvilket i så fald vil blive mere overkommeligt for virksomhederne.

Fjern-ID bliver obligatorisk på flere droner

Forslaget indeholder krav om:

- Direkte fjernidentifikation (Remote ID) på alle droner over 100 g, så observerede droner kan spores til den ansvarlige operatør.
- Krav om, at droner ikke må kunne anvendes uden aktiv Remote ID-funktionalitet.

FRI frygter, at disse krav vil tilføje ekstra "payload" til de lette droner, for at krav om remote-ID kan overholdes (3. parts hardware). Det kan bringe vægten over 250g, hvilket medfører krav om dronecertifikat, samt forbud mod at overflyve uvedkommende mennesker. Dette vil utvivlsomt begrænse brugen af små droner, i situationer, hvor de ellers ville være hensigtsmæssige at anvende. FRI vil gerne tilføje, at de fleste nyere droner allerede har en indbygget Remote-ID-løsning, og at det derfor bør være en 1-gangs-opgave at få aktiveret dette. I mange tilfælde vil en firmware opdatering være tilstrækkelig. FRI påpeger, at der er potentiale for en regelforenkling, såfremt Remote-ID bruges til at logge dronens placering fra centralt hold, fremfor den enkelte virksomhed kører log-bog over dens droner.

Ingen takeoff uden gyldigt operatør-ID (Ref.: s. 9)

Kommissionen vil indføre tekniske krav, der forhindrer start, hvis operatør-ID ikke er indtastet.

Dette medfører produktkrav til software i kommercielle droner og krav om brug af standardiserede IT-systemer. Droner uden godkendt ID vil i praksis ikke kunne tages i brug, og FRI forudser, at den daglige anvendelse af dronen kan blive ødelagt ved nedetid eller fejl i registrene, som følge af disse krav. I tilfælde af et fejlfrit teknisk system til registrering og flyvetilladelser, vurderer FRI, at kravet ikke burde være et problem, da det i forvejen er et krav at have operatør-ID.

Nye krav til dronehardware, software og cybersikkerhed

Sikkerhed i design ("security by design") (Ref.: s. 7)

Planen understreger, at droner på EU-markedet skal opfylde passende sikkerhedskrav.

Fra 2027 træder Cyber Resilience Act (CRA) i kraft, hvilket betyder:

- obligatoriske cybersikkerhedskrav for de fleste droner
- krav om anvendelse af "trusted chips" (sikring af teknisk hardware)
- krav om manipulations- og hackingssikrede komponenter

Dette kan øge omkostningerne ved dronekøb, særligt for droner fremstillet uden for EU, da dokumentationskravene for import skærpes. Kravene kan også reducere udvalget af godkendte modeller.

Selvom det i udgangspunktet vil være muligt at anvende ikke-Trusted droner, vil sådanne modeller få vanskeligere ved at blive godkendt til erhvervsflyvning hvilket kan medføre begrænset markedsadgang. Certificering kan derfor blive et konkurrenceparameter, hvilket er hensigten med ordningen, men kan have

en fordyrende effekt.

Geofencing, U-space og operationelle regler

Udvidet geo-awareness og fremtidig geofencing (Ref.: s. 6, 10-11)

Kommissionen vil udvide geo-awareness-kravene til alle droner over 100 g og forberede obligatorisk geofencing for at forhindre adgang til kritiske områder. Dette indebærer, at droner skal have avanceret software, som kan reagere på digitale signaler, der afgrænser restriktionszoner. Derudover stilles der krav om, at virksomheder holder deres droners zonedata løbende opdateret via U-space. Manglende overholdelse kan begrænse adgangen til erhvervsopgaver.

FRI ser en risiko for, at geofencing bliver meget omfattende, til en grad hvor det vil begrænse fordelene ved droneanvendelse i branchen.

FRI foreslår, at geofencing sker i følgeskab med krav til hurtigere og lempeligere dispensationsadgang. Yderligere vil det være nødvendigt for branchen, at en byggeplads med +50 m i omkreds fritages fra geofencing, hvis branchen skal kunne bruge droner effektivt.

U-space implementering (Ref.: s. 6, 10-11)

U-space er EU's digitale trafikstyringssystem for droner i lav højde. Det kan betragtes som et digitalt luftrum, hvor droner og myndigheder kan overvåge og koordinere droneaktivitet.

U-space består af fire kernefunktioner baseret på realtidskommunikation:

- **Netværksidentifikation:** myndigheder kan se drone-ID, operatør, position, rute og hensigt.
- **Lokationsbevidsthed:** droner reagerer automatisk på restriktionszoner, no-fly-zoner og beskyttede områder.
- **Flyveautorisering:** intentionen er, at flyvetilladelser skal gives automatisk og hurtigt for registrerede operatører.
- **Trafikinformation:** koordinering af lufttrafik samt risikoadvarsler.

FRI frygter, at U-space kan være særligt omkostningsfuldt for mindre droneaktører, der skal holde software og systemer ajour. FRI anbefaler derfor en undtagelse fra U-space for droner under 250g da dette er en kategori, der er særdeles skrøbelig over for hardwarekrav. Skubbes droner op i vægt over 250g, vil krav om certificering være en betydeligt fordyrende faktor i anvendelsen af droner.

Yderligere implikationer:

Ny Drone Security Toolbox (Ref.: s. 6-7)

Kommissionen vil etablere en fælles risikovurdering og en "security toolbox".

Det vil medføre minimumskrav til sensorer, dataforbindelser, kryptering, styrkede krav til importkontrol, og dokumentationspligt for hardwareleverandører.

Industripåvirkning (Ref.: s. 3-5)

Der er politisk ønske om at styrke europæisk produktion, bl.a. ved at favorisere EU-leverandører med sikkerhedscertificeringer.

Det kan medføre færre, mere regulerede producenter, og ikke-EU-producenter kan få en større regulatorisk byrde. Dette kan reducere konkurrencen og udvalget af droner, men samtidig øge sikkerheden.

Datadeling, overvågning og ansvarlighed (Ref.: s. 10-11)

Erhvervsmæssige droneflyvninger vil gradvist blive overvåget i realtid via U-space. Myndigheder vil få indsigt i droners anvendelse, og flyvedata kan opbevares i længere tid. Eventuelle overtrædelser kan spores direkte til operatør og drone.

Regelforenkling — der kommer også fordele (Ref.: s. 6)

Kommissionen foreslår reduceret behov for forudgående myndighedsgodkendelser og lettere adgang til flyvning både inden for og uden for synsvidde.

Forslaget sigter mod standardiserede processer og færre administrative byrder for at muliggøre hurtigere planlægning og reducere nationale forskelle.

ooo0ooo

Hvis I har behov for dialog eller uddybende bemærkninger, stiller vi os naturligvis til rådighed.