EUROPEAN COMMISSION
Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs
Single Market Enforcement
Notification of Regulatory Barriers

Notifikationsnummer : 2023/0761/ES (Spain)

# KONGELIGT DEKRET OM GODKENDELSE AF DEN NATIONALE SIKKERHEDSORDNING FOR 5G-NET OG -TJENESTER

Modtagelsesdato : 29/12/2023
Afslutning af status quo-periode : 02/04/2024 (closed)

## Message

Meddelelse 001

Kommissionens meddelelse - TRIS/(2023) 3739

Direktiv (EU) 2015/1535

Notifikation: 2023/0761/ES

Notifikation af et udkast fra en medlemsstat

Notification – Notification – Notifzierung – Нотификация – Oznámení – Notifikation – Γνωστοποίηση – Notificación – Teavitamine – Ilmoitus – Obavijest – Bejelentés – Notifica – Pranešimas – Paziņojums – Notifika – Kennisgeving – Zawiadomienie – Notificação – Notificare – Oznámenie – Obvestilo – Anmälan – Fógra a thabhairt

Does not open the delays - N'ouvre pas de délai - Kein Fristbeginn - Не се предвижда период на прекъсване - Nezahajuje prodlení - Fristerne indledes ikke - Καμμία έναρξη προθεσμίας - No abre el plazo - Viivituste perioodi ei avata - Määräaika ei ala tästä - Ne otvara razdoblje kašnjenja - Nem nyitja meg a késéseket - Non fa decorrere la mora - Atidėjimai nepradedami - Atlikšanas laikposms nesākas - Ma jiftaħx il-perijodi ta’ dewmien - Geen termijnbegin - Nie otwiera opóźnień - Não inicia o prazo - Nu deschide perioadele de stagnare - Nezačína oneskorenia - Ne uvaja zamud - Inleder ingen frist - Ní osclaíonn sé na moilleanna

MSG: 20233739.DA

1. MSG 001 IND 2023 0761 ES DA 29-12-2023 ES NOTIF

2. Spain

3A. Subdirección de Asuntos Industriales, Energéticos, de Transportes, Comunicaciones y de Medioambiente
D.G. de Mercado Interior y otras Políticas Comunitarias
Ministerio de Asuntos Exteriores, UE y Cooperación

3B. Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales.
Secretaría General de Telecomunicaciones y Ordenación de los Servicios de Comunicación Audiovisual.
Subdirección General de Ordenación de las Telecomunicaciones.
Ministerio de Transformación Digital

4. 2023/0761/ES - V00T - Teletjenester

5. KONGELIGT DEKRET OM GODKENDELSE AF DEN NATIONALE SIKKERHEDSORDNING FOR 5G-NET OG -TJENESTER

6. 5G-net og -tjenester til elektroniske kommunikation

Telekommunikationsudstyr.

7.

8. Reglen består af en forklarende del, en enkelt artikel om godkendelse af ENS5G (national sikkerhedsordning for 5G), to supplerende bestemmelser samt fire afsluttende bestemmelser.
Den ENS5G, der skal godkendes, består af 33 artikler fordelt på otte kapitler og tre bilag.
I begrundelsen forklares årsagerne til reglens vedtagelse og de artikler i det kongelige lovdekret, der er under udarbejdelse.
I den enkelte artikel godkendes den nationale sikkerhedsordning for 5G-net og -tjenester.
I den første tillægsbestemmelse fastsættes det, at regeringen ved kongeligt dekret, på forslag fra ministeriet for digital omstilling og efter rapport fra det nationale sikkerhedsråd, skal revidere den nationale sikkerhedsordning for 5G-net og -tjenester, når omstændighederne kræver det, og under alle omstændigheder hvert fjerde år.
I den anden supplerende bestemmelse fastsættes det, at kongeligt lovdekret 7/2022 af 29. marts 2022 og ENS5G skal finde anvendelse på generationer af elektronisk kommunikation efter den femte generation, så længe der ikke foreligger nogen specifik regel for disse.
I den første afsluttende bestemmelse om kompetence fastsættes det, at det kongelige dekret og den ordning, den godkender, udstedes i henhold til bestemmelserne i artikel 149, stk. 1, nr. 21, og artikel 149, stk. 1, nr. 29, i den spanske forfatning, som tildeler staten enekompetence i spørgsmål om henholdsvis det generelle telekommunikationssystem og spørgsmål om offentlig sikkerhed.
I den anden afsluttende bestemmelse erklæres lov 11/2022 af 28. juni 2022 om generel telekommunikation og dens gennemførelsesbestemmelser for at være af supplerende anvendelse, og det anføres, at i alle spørgsmål, der ikke er reguleret i denne lovgivning, skal kongeligt lovdekret 12/2018 af 7. september 2018 om sikkerhed i net og informationssystemer og lov 8/2011 af 28. april 2011 om indførelse af foranstaltninger til beskyttelse af kritisk infrastruktur samt deres respektive gennemførelsesbestemmelser være af supplerende anvendelse.
Den tredje afsluttende bestemmelse om reguleringsmæssig udvikling bemyndiger lederen af ministeriet for digital omstilling til at udarbejde bestemmelserne i dette kongelige dekret og den ordning, som den godkender, og til ved bekendtgørelse at ændre indholdet af bilagene i overensstemmelse med den teknologiske udvikling, godkendelsen af nye tekniske standarder og certificeringsordninger for telekommunikationsudstyr og tilhørende produkter såvel som udviklingen inden for forskellige konfigurationer og tekniske parametre for 5G-net og -tjenester og fremtidige generationer af elektronisk kommunikation.
Den fjerde og sidste bestemmelse fastsætter, at reglen træder i kraft dagen efter dens offentliggørelse i den spanske statstidende.
For så vidt angår indholdet af den ENS5G, der godkendes:
Artikel 1 fastslår, at reglen udstedes til gennemførelse af kongeligt lovdekret 7/2022 af 29. marts 2022, navnlig med henblik på anvendelsens af dekretets kapitel IV.
Artikel 2 henviser til reglens formål, som allerede er analyseret.
Artikel 3 fastslår, at definitionerne i kongeligt lovdekret 7/2022 af 29. marts 2022, lov nr. 11/2022 af 28. juni 2022 om generel telekommunikation og den europæiske kodeks for elektronisk kommunikation skal finde anvendelse.
Artikel 4 fastslår, at reglen finder anvendelse på 5G-operatører, -leverandører og -erhvervsbrugere, der har ret til at bruge det offentlige radiodomæne til at installere, udrulle eller drive et privat 5G-net eller til at levere 5G-tjenester til professionelle formål eller til selvforsyning.
Artikel 5 udpeger de minimumselementer, den infrastruktur og de ressourcer, der udgør et 5G-net til elektronisk kommunikation, og henviser til bilag I for en detaljeret beskrivelse af disse. Den beskriver også de kritiske elementer i et 5G-net, der som hovedregel skal være placeret på det nationale område (herunder eventuelle undtagelser).
Artikel 6 henviser til den overordnede sikkerhedshåndtering i henhold til den nationale og internationale EU-lovgivning, der er eller måtte blive godkendt, og som i kraft af en helhedsorienteret tilgang pålægger de forpligtede parter at foretage en analyse af de sårbarheder, trusler og risici, der påvirker dem som økonomiske aktører og af de forskellige komponenter, samt en hensigtsmæssig overordnet risikostyring på grundlag af egnede teknikker og foranstaltninger med henblik på at begrænse eller eliminere disse risici og nå det endelige mål om en sikker udnyttelse og drift af 5G-net og -tjenester.

Artikel 7 understreger, at risikoanalyse og -styring er en væsentlig del af sikkerhedsprocessen og derfor bør være en fortløbende indsats, der løbende opdateres.
Artikel 8 henviser til løbende overvågning og periodisk revurdering.
Artikel 9 fastslår, at den nationale risikoanalyse er som beskrevet i bilag II og at den er gennemført under hensyntagen til en række elementer såsom oplysninger indsamlet fra de forpligtede parter, undersøgelse af sårbarheder i forbindelse med forsyningskæden for 5G-net og -tjenester, vurdering af graden af leverandørafhængighed, risikoen for afbrydelse af forsyningen som følge af økonomiske, erhvervsmæssige eller kommercielle forhold, der påvirker leverandørerne, eller vurdering af effektiviteten af de anvendte sikkerhedsforanstaltninger.
I artikel 10 vedrørende den nationale risikostyring fastslås det, at kriterierne, kravene, betingelserne og fristerne for de forpligtede parters udformning og gennemførelse af teknikker og foranstaltninger til risikobegrænsning er dem, der er angivet i bilag III.
Artikel 11 udbygger bestemmelserne i artikel 14 i kongeligt lovdekret nr. 7/2022 af 29. marts 2022 for så vidt angår den procedure og de aspekter, der skal vurderes af ministerrådet med henblik på klassificering af leverandører som højrisikoleverandører, og de elementer, der skal tages i betragtning ved bestilling af eventuel udskiftning af udstyr, produkter og tjenester, der leveres af de pågældende leverandører. I overensstemmelse med bestemmelserne i det førnævnte kongelige lovdekret anføres det ligeledes, at højrisikoleverandører, hvis telekommunikationsudstyr, hardware, software eller tilknyttede tjenester udelukkende anvendes i private 5G-net eller til levering af 5G-tjenester i henhold til selvforsyning, skal klassificeres som mellemrisikoleverandører.
I artikel 12 vedrørende bestemmelsen af steder, hvor udstyr fra leverandører, der er klassificeret som højrisikoleverandører, ikke må installeres, fastsættes det, at det nationale sikkerhedsråd efter indstilling fra ministeriet for digital omstilling kan fastlægge de steder, områder og centre, hvor udstyr fra leverandører, der er klassificeret som højrisikoleverandører, ikke må installeres. Ved installation, ændring eller tilpasning af radiostationer, der leverer dækning til disse steder, områder og centre, skal 5G-operatørerne anmode om tilladelse fra ministeriet for digital omstilling.
Artikel 13 forpligter 5G-operatørerne til at udarbejde en diversificeringsstrategi for forsyningskæden og til at benytte transmissionsudstyr i adgangsnettet, som leveres af mindst to forskellige leverandører. Den indeholder desuden kriterier, som ministerrådet skal tage hensyn til for at afgøre, om det er muligt at opretholde en enkelt leverandør, i tilfælde af at antallet af leverandører måtte blive reduceret som følge af fusioner. Derudover angiver den forudsætningerne og proceduren for, hvorledes ministeriet for digital omstilling kan ændre en 5G-operatørs strategi for diversificering af forsyningskæden.
Artikel 14 fokuserer på den risikoanalyse, som 5G-operatører skal udføre i forhold til alle de i bilag I nævnte elementer, infrastrukturer og ressourcer i nettet, opregner de faktorer, der skal tages i betragtning, og pålægger operatørerne at indhente oplysninger fra deres leverandører om den sikkerhedspraksis og de sikkerhedsforanstaltninger, de har anvendt i forbindelse med de produkter og tjenester, de har leveret og at foretage en prioritering og hierarkisering af risici i henhold til visse parametre, som ligeledes er opregnet. Senest den 1. oktober 2024 skal 5G-operatørerne fremsende en risikoanalyse og derefter hvert andet år.
Artikel 15 om 5G-leverandørers risikoanalyse forpligter dem til at analysere risikoen ved det telekommunikationsudstyr, den hardware og software og de tilknyttede tjenester, der er involveret i driften af deres 5G-net eller i leveringen af deres 5G-tjenester, og til efter anmodning at forelægge en sådan analyse for ministeriet. Hvis der er tale om leverandører, der er klassificeret som højrisiko- eller mellemrisikoleverandører, skal analysen forelægges inden for seks måneder efter den pågældende klassificering og derefter hvert andet år.
Artikel 16 vedrørende 5G-erhvervsbrugeres risikoanalyse pålægger dem at levere denne risikoanalyse til ministeriet for digital omstilling, såfremt de er forpligtet til det.
Artikel 17 bemyndiger ministeriet for digital omstilling til at indsamle de for risikoanalysen nødvendige oplysninger fra de forpligtede parter og definerer det som en alvorlig overtrædelse, hvis sådanne oplysninger ikke leveres inden for 15 arbejdsdage. Oplysningerne betragtes som fortrolige og må ikke anvendes til andre formål end opfyldelsen af de mål og forpligtelser, der er fastsat i kongeligt lovdekret 7/2022 af 29. marts 2022, i ENS5G og i de love, der udstedes til gennemførelse af begge bestemmelser.
Artikel 18 erklærer den generelle pligt for alle forpligtede parter til at styre sikkerhedsrisici.
Artikel 19 fokuserer på 5G-operatørers sikkerhedsstyring, opstilling af forpligtelser for alle operatører (f.eks. at vedtage beredskabsplaner og -foranstaltninger, at overholde europæiske standarder eller tekniske specifikationer og certificeringsordninger, at underkaste sig en sikkerhedsaudit for egen regning eller at kræve, at deres leverandører overholder sikkerhedsstandarderne) og yderligere forpligtelser for de operatører, der ejer eller driver kritiske elementer i

et offentligt 5G-net (f.eks. forbud mod anvendelse af udstyr fra højrisikoleverandører i kritiske netelementer eller på visse steder, områder og centre). 5G-operatører skal senest den 1. oktober 2024 og derefter hvert andet år forelægge ministeriet for digital omstilling en beskrivelse af de tekniske og organisatoriske foranstaltninger, der er udarbejdet og implementeret med henblik på at styre og afbøde risici. Derudover skal 5G-operatører, der ejer eller driver kritiske elementer i et offentligt 5G-net fremsende en diversificeringsstrategi for forsyningskæden til ministeriet for digital omstilling senest den 1. oktober 2024 og derefter hver gang, strategien ændres. Oplysninger om status for strategiens gennemførelse skal indsendes senest den 1. oktober hvert år.
Artikel 20 om 5G-leverandørers sikkerhedsstyring indeholder en liste over forpligtelser, herunder gennemførelse af en sikkerhedsaudit af deres udstyr, produkter og tjenester, oplysninger om tredjeparters mulige interferens i udformningen, driften og funktionen af deres udstyr, produkter og tjenester og samarbejde med 5G-operatører og -erhvervsbrugere ved at tilvejebringe oplysninger og certificere overholdelse af standarder og certificeringer. 5G-leverandører skal udarbejde en rapport om de tekniske og organisatoriske foranstaltninger, der er udarbejdet og implementeret med henblik på at styre og afbøde risici og på anmodning fremlægge denne for ministeriet. Hvis der er tale om leverandører, der er klassificeret som højrisiko- eller mellemrisikoleverandører, skal rapporten forelægges inden for 6 måneder efter den pågældende klassificering og derefter hvert andet år.
Artikel 21 om sikkerhedsstyring af 5G-erhvervsbrugere fastslår, at disse ikke må benytte telekommunikationsudstyr, transmissionssystemer, koblings- eller routingudstyr og andre ressourcer i de kritiske netelementer, som tillader transport af signaler, hardware, software eller tilknyttede tjenester fra leverandører, der er blevet klassificeret som mellemrisikoleverandører. Derudover skal brugerne efter anmodning give ministeriet for digital omstilling en beskrivelse af de tekniske og organisatoriske foranstaltninger, der er udarbejdet og implementeret med henblik på at styre og afbøde risici.
Artikel 22 om offentlige myndigheders sikkerhedsstyring fastslår, at offentlige myndigheder af hensyn til den nationale sikkerhed ikke må anvende udstyr, produkter og tjenester, der leveres af højrisiko- eller mellemrisikoleverandører, i forbindelse med installation, udrulning og drift af 5G-net, hvad enten de er offentlige eller private, eller ved levering af 5G-tjenester, hvad enten de er offentligt tilgængelige eller til selvforsyning.
Artikel 23 fastslår, at de forpligtede parter, i overensstemmelse med de forpligtelser, der er fastsat i de foregående artikler, skal tage hensyn til og overholde det, der er fastsat i kongeligt lovdekret 7/2022 af 29. marts 2022, i ENS5G og i de love, der udstedes til gennemførelse af begge bestemmelser.
Artikel 24 bemyndiger ministeriet for digital omstilling til at indsamle de for risikostyringen nødvendige oplysninger fra de forpligtede parter og definerer det som en alvorlig overtrædelse, hvis sådanne oplysninger ikke leveres inden for 15 arbejdsdage. Oplysningerne betragtes som fortrolige og må ikke anvendes til andre formål end opfyldelsen af de mål og forpligtelser, der er fastsat i kongeligt lovdekret 7/2022 af 29. marts 2022, i ENS5G og i de love, der udstedes til gennemførelse af begge bestemmelser.
Artikel 25 fastslår, at alle forpligtede parter, såvel som de offentlige myndigheder, producenter, importører, distributører og dem, der markedsfører og sælger terminaludstyr og enheder, der skal tilsluttes et 5G-net og kunne levere 5G-tjenester, skal samarbejde og indsende de oplysninger, der er nødvendige for at ændre og implementere ENS5G.
Artikel 26 fastslår at anvendelsen af et bestemt udstyr, system, program eller en tjeneste ved bekendtgørelse fra lederen af ministeriet for digital omstilling kan gøres betinget af forudgående certificering i henhold til Europa-Parlamentets og Rådets forordning (EU) 2019/881 af 17. april 2019 om cybersikkerhed eller i henhold til certificeringsordninger og tekniske standarder for certificering af 5G-udstyr og -produkter, der kan godkendes på europæisk eller internationalt plan.
Artikel 27 fastsætter, at reglen finder anvendelse, uden at dette berører de udenlandske investeringer og konkurrencelovgivningen.
Artikel 28 om terminaludstyr fastsætter, at fremstilling, import, distribution, markedsføring og salg af terminaludstyr og enheder, der skal tilsluttes et 5G-net og kunne levere 5G-tjenester, er betinget af overholdelse af sikkerhedskravene til digitale produkter og de gældende væsentlige cybersikkerhedskrav, der er vedtaget i overensstemmelse med EU-lovgivningen, navnlig med hensyn til beskyttelse af personoplysninger, privatlivets fred og beskyttelse mod svig.
Artikel 29 henviser til det internationale samarbejde, der skal udbygges via ministeriet for digital omstilling, navnlig på EU-plan.
Artikel 30 henviser til ministeriet for digital omstillings kompetence i forbindelse med gennemførelsen af ENS5G. Ministeriet bør koordinere med de andre organer med ansvar for cybersikkerhed og kritisk infrastruktur for at sikre en konsekvent gennemførelse af ENS5G.

Artikel 31 udspecificerer de beføjelser i forbindelse med gennemførelsen af ENS5G, der tilkommer ministeriet for digital omstilling, herunder f.eks. udvikling, konkretisering og detaljering af indholdet af ENS5G, iværksættelse af audit med henblik på at verificere og overvåge overholdelsen af de pålagte forpligtelser samt tildeling af offentlig støtte.
Artikel 32 tillægger ministeriet for digital omstilling alle beføjelser i forbindelse med kontrolfunktionen.
Artikel 33 om sanktionsordningen henviser til bestemmelserne i artikel 30 og 31 i kongeligt lovdekret 7/2022 af 29. marts 2022.
Bilag I beskriver de elementer, den infrastrukturer og de ressourcer, der udgør et 5G-net.
Bilag II indeholder den nationale risikoanalyse.
Bilag III fastsætter den nationale risikostyring.

9. Femte generation af mobil kommunikation eller 5G-mobilkommunikation repræsenterer et nyt paradigme for elektronisk kommunikation med et stort forandringspotentiale til gavn for samfundet og økonomien, da det åbner mulighed for at indarbejde nye funktionaliteter, der vil få stor betydning, f.eks. databehandling, og det giver mulighed for at oprette virtuelle net med lav latenstid og levere tjenester med høj merværdi inden for områder som medicin, transport og energi.
Derfor opfordrer såvel EU som Spanien til en hurtig udrulning af 5G-net og gennemførelse af projekter, der demonstrerer deres nytteværdi for forskellige sektorer gennem leveringen af 5G-tjenester.
5G-net og -tjenester har komparative sikkerhedsfordele i forhold til tidligere generationer. De udgør imidlertid også specifikke risici, der bl.a. skyldes deres mere komplekse, åbne og opdelte netarkitektur og deres evne til at transportere enorme mængder data og muliggøre samtidig interaktion mellem flere personer og ting. Deres sammenkobling med andre net og truslernes transnationale karakter har indflydelse på deres sikkerhed, og den forventede udbredte brug af disse net til væsentlige økonomiske og samfundsmæssige funktioner vil øge den potentielle effekt af de sikkerhedshændelser, de udsættes for.
Disse nye særskilte sikkerhedsrisici ved 5G-mobilkommunikation blev reguleret ved kongeligt lovdekret nr. 7/2022 af 29. marts 2022 om krav til sikring af femte generation af elektroniske kommunikationsnet og -tjenester, som fuldt ud indarbejder Europa-Kommissionens henstilling (EU) 2019/534 af 26. marts 2019 om cybersikkerheden i forbindelse med 5G-net samt de anbefalinger, som Europa-Kommissionens meddelelse af 29. januar 2020 om en EU-værktøjskasse til udrulning af sikre 5G-net i EU (COM/2020/50 final) fremsatte over for medlemsstaterne med hensyn til brugen af værktøjskassen.
Det førnævnte kongelige lovdekret 7/2022 af 29. marts 2022 indeholder bestemmelser om den reguleringsmæssige udvikling i form af den nationale sikkerhedsordning for 5G-net og -tjenester (ENS5G).
I overensstemmelse med artikel 5, stk. 3, i førnævnte kongelige lovdekret skal ENS5G omfatte en samlet sikkerhedsmæssig behandling af 5G-net og -tjenester under hensyntagen til de bidrag, som de enkelte aktører i 5G-værdikæden yder, samt regler, anbefalinger og tekniske standarder fra EU, Den Internationale Telekommunikationsunion (ITU) og andre internationale organisationer for at garantere det endelige mål om sikker brug og drift af 5G-net og -tjenester i Spanien.
Artikel 20 i det kongelige lovdekret fastlægger, at ENS5G for at opretholde en sikker drift af 5G-nettet og -tjenesterne skal gennemføre en national risikoanalyse af sikkerheden ved 5G-net og -tjenester og identificere, udspecificere og udarbejde foranstaltninger til at afbøde og styre de analyserede risici.
Endelig skal ENS5G i overensstemmelse med artikel 21 i det kongelige lovdekret godkendes af regeringen ved kongeligt dekret, på forslag fra ministeriet for digital omstilling efter indstilling fra det nationale sikkerhedsråd.
Med denne regel godkendes ENS5G, som videreudvikler bestemmelserne i kongeligt lovdekret 7/2022 af 29. marts 2022 om krav til sikring af femte generation af elektroniske kommunikationsnet og -tjenester.

10. Henvisninger til grundtekster:

11. Nej

12.

13. Nej

14. Nej

15. Ja

16.
TBT-aspekt: Nej

SPS-aspekt: Nej

**********
Europa-Kommissionen
Kontaktadresse Direktiv (EU) 2015/1535
email: grow-dir2015-1535-central@ec.europa.eu