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

Teatise number : 2023/0761/ES (Spain)

KUNINGLIK DEKREET, MILLEGA KIIDETAKSE HEAKS 5G-VÕRKUDE JA -TEENUSTE RIIKLIK TURVASÜSTEEM

Teatise saamise kuupäev : 29/12/2023
Ooteaja lõpp : 02/04/2024 (closed)

Message

Sõnum 001

Komisjoni teade - TRIS/(2023) 3739

Direktiiv (EL) 2015/1535

Teavitamine: 2023/0761/ES

Liikmesriigi teade teksti kavandi kohta

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.ET

1. MSG 001 IND 2023 0761 ES ET 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 - Telekommunikatsioon

5. KUNINGLIK DEKREET, MILLEGA KIIDETAKSE HEAKS 5G-VÕRKUDE JA -TEENUSTE RIIKLIK TURVASÜSTEEM

6. 5G elektroonilised sidevõrgud ja -teenused

Telekommunikatsiooniseadmed.

7.

8. Määrus koosneb selgitavast osast, ühest artiklist, millega kiidetakse heaks ENS5G (riiklik 5G turvasüsteem), kaks täiendavat sätet ja 4 lõppsätet.
Heaks kiidetav ENS5G koosneb 33 artiklist, mis on jagatud kaheksaks peatükiks ja kolmeks lisaks.
Seletuskirjas selgitatakse määruse vastuvõtmise põhjuseid ja väljatöötatavaid kuningliku dekreetseaduse artikleid.
Artiklis kiidetakse heaks 5G-võrkude ja -teenuste riiklik turvasüsteem.
Esimese lisasätte kohaselt vaatab valitsus pärast riikliku julgeolekunõukogu aruannet kuningliku dekreediga 5G-võrkude ja -teenuste riikliku turvasüsteemi läbi, kui asjaolud seda nõuavad, ja igal juhul iga nelja aasta tagant.
Teises täiendavas sättes on sätestatud, et 29. märtsi 2022. aasta kuninglikku dekreetseadust 7/2022 ja ENS5G kohaldatakse elektroonilise side põlvkondade suhtes pärast viiendat põlvkonda, ilma et nende jaoks erieeskirju oleks kehtestatud.
Pädevuse esimese viimase sätte kohaselt antakse kuninglik dekreet ja sellega heaks kiidetud kord välja Hispaania põhiseaduse artikli 149 lõike 1 punkti 21 ja artikli 149 lõike 1 punkti 29 alusel, mis annavad riigile ainupädevuse vastavalt üldise telekommunikatsioonisüsteemi ja avaliku julgeoleku küsimustes.
Teises viimases sättes kuulutatakse täiendavaks kohaldamiseks 28. juuni 2022. aasta üldtelekommunikatsiooniseadus 11/2022 ja selle rakendusmäärused ning sätestatakse, et kõigis küsimustes, mida nimetatud õigusaktid ei reguleeri, kohaldatakse täiendavalt 7. septembri 2018. aasta kuninglikku dekreetseadust 12/2018 võrkude ja infosüsteemide turvalisuse kohta ning 28. aprilli 2011. aasta seadust 8/2011, millega kehtestatakse meetmed elutähtsa taristu kaitseks, ning nende vastavaid rakendusmäärusi.
Kolmas õigusnormide arengut käsitlev lõppsäte võimaldab digiülemineku ministeeriumi juhil töötada välja käesoleva kuningliku dekreedi sätted ja selle süsteemi ning muuta korraldusega lisade sisu vastavalt tehnoloogia arengule, telekommunikatsiooniseadmete ja nendega seotud toodete uute tehniliste standardite ja sertifitseerimissüsteemide heakskiitmisele ning 5G-võrkude ja -teenuste ning tulevaste elektroonilise side põlvkondade erinevate konfiguratsioonide ja tehniliste parameetrite väljatöötamisele.
Neljas lõppsäte näeb ette, et määrus jõustub järgmisel päeval pärast selle avaldamist ametlikus väljaandes.
Heaks kiidetud ENS5G sisu osas:
Artiklis 1 on sätestatud, et määrus antakse välja 29. märtsi 2022. aasta kuningliku dekreetseaduse 7/2022 rakendamiseks, eelkõige selle IV peatüki kohaldamiseks.
Artiklis 2 viidatakse määruse eesmärkidele, mida on juba analüüsitud.
Artiklis 3 on sätestatud, et kasutatakse 29. märtsi 2022. aasta kuninglikus dekreetseaduses 7/2022, 28. juuni 2022. aasta seaduses 11/2022 üldise telekommunikatsiooni kohta ja Euroopa elektroonilise side seadustikus sätestatud mõisteid.
Artiklis 4 on sätestatud, et määrust kohaldatakse 5G operaatorite, 5G tarnijate ja 5G ärikasutajate suhtes, kellel on õigus kasutada avalikku raadioomandit 5G-eravõrgu paigaldamiseks, kasutuselevõtuks või käitamiseks või 5G-teenuste osutamiseks ametialastel eesmärkidel või iseteeninduseks.
Artiklis 5 määratakse kindlaks minimaalsed elemendid, taristu ja ressursid, mis moodustavad 5G elektroonilise sidevõrgu, viidates nende üksikasjaliku kirjelduse osas I lisale. Selles sätestatakse ka 5G-võrgu kriitilised elemendid, mis peavad üldjuhul asuma riigi territooriumil (sealhulgas võimalikud erandid).
Artiklis 6 osutatakse turvalisuse terviklikule käsitlemisele vastavalt rahvusvahelistele ühenduse ja siseriiklikele õigusaktidele, mis on heaks kiidetud või mida võib heaks kiita, nõudes kohustatud isikutelt tervikliku meetodi abil nende kui majandussubjektide haavatavuste, ohtude ja riskide ning eri komponentide analüüsimist, samuti nende riskide piisavat ja terviklikku juhtimist tehnikate ja meetmete abil, mis on asjakohased nende leevendamiseks või kõrvaldamiseks ning 5G-võrkude ja -teenuste turvalise kasutamise ja käitamise lõppeesmärgi saavutamiseks.
Artiklis 7 rõhutatakse, et riskianalüüs ja -juhtimine on julgeolekuprotsessi oluline osa ning see peaks olema pidev tegevus, mida pidevalt ajakohastatakse.
Artiklis 8 viidatakse pidevale järelevalvele ja perioodilisele ümberhindamisele.
Artiklis 9 on sätestatud, et riigi tasandi riskianalüüs on sätestatud II lisas ja selle tegemisel on võetud arvesse mitmesuguseid elemente, nagu kohustatud isikutelt kogutud teave, 5G-võrkude ja -teenuste tarneahelaga seotud haavatavuste uurimine, tarnijate sõltuvuse taseme hindamine, tarnijaid mõjutavate majanduslike, äriliste või äriliste

asjaolude tõttu tarnimise katkemise oht või rakendatavate turvameetmete tõhususe hindamine.
Artiklis 10, mis käsitleb riskijuhtimist riiklikul tasandil, on sätestatud, et kriteeriumid, nõuded, tingimused ja tähtajad, mille jooksul kohustatud isikud peavad riskimaandamistehnikaid ja -meetmeid kavandama ja rakendama, on sätestatud III lisas.
Artikliga 11 arendatakse edasi 29. märtsi 2022. aasta kuningliku dekreetseaduse 7/2022 artikli 14 sätteid seoses menetluste ja aspektidega, mida ministrite nõukogu peab hindama tarnijate kõrgeks riskiks liigitamisel, ning elementide osas, mida tuleb arvesse võtta nende tarnijate pakutavate seadmete, toodete ja teenuste võimaliku asendamise tellimisel. Samuti on eespool nimetatud kuningliku dekreetseaduse sätete kohaselt märgitud, et suure riskiga teenuseosutajad, kelle osutatavaid telekommunikatsiooniseadmeid, riist-, tarkvara või kõrvalteenuseid kasutatakse üksnes ja eranditult 5G eravõrkudes või 5G-teenuste osutamiseks iseteeninduse raames, liigitatakse keskmise riskiga tarnijateks.
Artiklis 12, mis käsitleb selliste kohtade kindlaksmääramist, kuhu ei tohi paigaldada kõrge riskitasemega tarnijate seadmeid, on sätestatud, et riiklik julgeolekunõukogu võib pärast digiülemineku ministeeriumi aruannet määrata kindlaks asukohad, piirkonnad ja keskused, kuhu ei tohi paigaldada suure riskiga tarnijate seadmeid. Nende kohtade, piirkondade ja keskuste levialaga raadiojaamade paigaldamiseks, muutmiseks või kohandamiseks peavad 5G operaatorid taotlema luba digiülemineku ministeeriumilt.
Artikliga 13 kohustatakse 5G ettevõtjaid kavandama tarneahela mitmekesistamise strateegiat ja omama juurdepääsuvõrku ülekandeseadmeid, mida pakuvad vähemalt kaks eri tarnijat. Samuti on selles sätestatud kriteeriumid, mida ministrite nõukogu peab arvesse võtma, et otsustada, kas on võimalik säilitada üksainus tarnija, kui tarnijate arv ühinemiste tõttu väheneb. Lisaks on selles esitatud eeldused ja kord, mille kohaselt saab digiülemineku ministeerium muuta 5G operaatori tarneahela mitmekesistamise strateegiat.
Artiklis 14 keskendutakse riskianalüüsile, mida teevad 5G ettevõtjad I lisas esitatud võrgu kõigi elementide, infrastruktuuri ja ressursside kohta, loetletakse tegurid, mida tuleb arvesse võtta, ning kohustatakse ettevõtjaid koguma oma tarnijatelt turvatavasid ja -meetmeid, mida nad on neile tarnides ja teenuste osutamisel kasutanud, ning lisama prioriteetide seadmise ja riskide hierarhia vastavalt teatavatele loetletud parameetritele. Hiljemalt 1. oktoobriks 2024 peavad 5G ettevõtjad esitama riskianalüüsi ja kordama seda seejärel iga kahe aasta tagant.
Artiklis 15, mis käsitleb 5G tarnijate tehtavat riskianalüüsi, nõutakse 5G-võrkude toimimise või käitamisega või 5G-teenuste osutamisega seotud telekommunikatsiooniseadmete, riist- ja tarkvara ning kõrvalteenustega seotud riskide analüüsimist ning nimetatud analüüsi tegemist ministeeriumile taotluse korral. Suure või keskmise riskiga tarnijate puhul esitatakse analüüs kuue kuu jooksul pärast klassifitseerimist ja seejärel iga kahe aasta tagant.
Artiklis 16, mis käsitleb 5G ärikasutajate riskianalüüsi, nõutakse, et see riskianalüüs esitataks digiülemineku ministeeriumile, kui vastavad kasutajad peavad seda tegema.
Artikkel 17 võimaldab digiülemineku ministeeriumil koguda kohustatud isikutelt riskianalüüsiks vajalikku teavet ja liigitab sellise teabe esitamata jätmise 15 tööpäeva jooksul tõsiseks rikkumiseks. Teavet käsitatakse konfidentsiaalsena ja seda ei tohi kasutada muul eesmärgil kui 29. märtsi 2022. aasta kuninglikus dekreetseaduses 7/2022, ENS5G-s ja mõlema sätte rakendamiseks välja antud õigusaktides sätestatud eesmärkide ja kohustuste täitmiseks.
Artiklis 18 sätestatakse kõigi kohustatud isikute üldine kohustus hallata turvariske.
Artiklis 19 keskendutakse turvalisuse haldamisele 5G operaatorite poolt, kõigi operaatorite kohustustele (nt võtta vastu situatsiooniplaanid ja -meetmed, järgida Euroopa standardeid või tehnilisi spetsifikatsioone ja sertifitseerimissüsteeme, läbida omal kulul turvaaudit või nõuda oma tarnijatelt turvastandardite järgimist) ning lisakohustustele operaatoritele, kes omavad või käitavad avaliku 5G-võrgu kriitilisi elemente (näiteks keeld kasutada suure riskiga tarnijate seadmeid kriitilistes võrguelementides või teatavates kohtades, piirkondades ja keskustes). 5G ettevõtjad peavad esitama digiülemineku ministeeriumile riskide juhtimiseks ja maandamiseks kavandatud ja rakendatud tehniliste ja korralduslike meetmete kirjelduse 1. oktoobriks 2024 ja seejärel iga kahe aasta tagant. Lisaks peavad 5G operaatorid, kes omavad või kasutavad 5G avaliku võrgu kriitilisi elemente, esitama digiülemineku ministeeriumile tarneahela mitmekesistamise strateegia 1. oktoobriks 2024 ja seejärel iga kord, kui seda muudetakse. Teave selle strateegia rakendamise seisu kohta tuleb esitada iga aasta 1. oktoobriks.
Artiklis 20, mis käsitleb turvalisuse haldamist 5G tarnijate poolt, on loetletud kohustused, sealhulgas nende seadmete, toodete ja teenuste turvaaudit, mis annab teavet kolmandate isikute võimalike häirete kohta oma seadmete, toodete ja teenuste kavandamisse, toimimisse ja toimimisse ning teeb koostööd 5G operaatorite ja 5G ärikasutajatega, esitades teavet ning kinnitades standardite ja sertifikaatide järgimist. 5G tarnijad peavad koostama aruande riskide juhtimiseks ja maandamiseks kavandatud ja rakendatud tehniliste ja korralduslike meetmete kohta ning esitama nimetatud aruande

ministeeriumile taotluse korral. Suure või keskmise riskiga tarnijate puhul esitatakse aruanne kuue kuu jooksul pärast klassifitseerimist ja seejärel iga kahe aasta tagant.
Artiklis 21, mis käsitleb turvahaldust 5G ärikasutajate poolt, on sätestatud, et neid ei tohi kasutada elutähtsates võrguelementides telekommunikatsiooniseadmetes, ülekandesüsteemides, lülitus- või marsruutimisseadmetes ja muudes ressurssides, mis võimaldavad keskmise riskiga tarnijatel edastada signaale, riist-, tarkvara või abiteenuseid. Lisaks peavad kasutajad esitama digiülemineku ministeeriumile taotluse korral riskide juhtimiseks ja maandamiseks kavandatud ja rakendatud tehniliste ja korralduslike meetmete kirjelduse.
Artiklis 22, mis käsitleb julgeolekuhaldust haldusasutuste poolt, on sätestatud, et riigi julgeoleku huvides ei tohi avaliku või erasektori 5G-võrkude paigaldamisel, kasutuselevõtmisel ja käitamisel või 5G-teenuste osutamisel, olenemata sellest, kas need on üldkasutatavad või iseteeninduseks, kasutada suure või keskmise riskiga tarnijate pakutavaid seadmeid, tooteid ja teenuseid.
Artiklis 23 on sätestatud, et kooskõlas eelmistes artiklites sätestatud kohustustega võtavad kohustatud isikud arvesse ja kohaldavad seda, mis on sätestatud 29. märtsi 2022. aasta kuninglikus dekreetseaduses 7/2022, ENS5G-s ja mõlema sätte rakendamiseks välja antud õigusaktides.
Artikkel 24 võimaldab digiülemineku ministeeriumil koguda kohustatud isikutelt riskianalüüsiks vajalikku teavet ja liigitab sellise teabe esitamata jätmise 15 tööpäeva jooksul tõsiseks rikkumiseks. Teavet käsitatakse konfidentsiaalsena ja seda ei tohi kasutada muul eesmärgil kui 29. märtsi 2022. aasta kuninglikus dekreetseaduses 7/2022, ENS5G-s ja mõlema sätte rakendamiseks välja antud õigusaktides sätestatud eesmärkide ja kohustuste täitmiseks.
Artiklis 25 on sätestatud, et kõik kohustatud isikud, samuti haldusasutused, tootjad, importijad, levitajad ja need, kes viivad turule ja müüvad lõppseadmeid ja seadmeid 5G-võrguga ühendamiseks ja 5G-teenuste osutamiseks, peavad tegema koostööd ja esitama ENS5G muutmiseks ja rakendamiseks vajaliku teabe.
Artiklis 26 on sätestatud, et digiülemineku ministeeriumi juhi korraldusel võib konkreetse seadme, süsteemi, programmi või teenuse kasutamise tingimuseks seada eelneva sertifitseerimise vastavalt Euroopa Parlamendi ja nõukogu 17. aprilli 2019. aasta määrusele (EL) 2019/881 küberturvalisuse kohta või sertifitseerimiskavadele ja tehnilistele standarditele 5G-seadmete ja -toodete sertifitseerimiseks, mida võib heaks kiita Euroopa või rahvusvahelisel tasandil.
Artiklis 27 on sätestatud, et määrust kohaldatakse, ilma et see piiraks välisinvesteeringute ja konkurentsiõiguse kohaldamist.
Lõppseadmeid käsitlevas artiklis 28 on sätestatud, et 5G-võrguga ühendamiseks ja 5G-teenuste osutamiseks vajalike lõppseadmete ja seadmete tootmine, import, levitamine, turule laskmine ja müük sõltub digitoodete turvanõuete ja küberturvalisusega seotud kohaldatavate oluliste nõuete järgimisest, mis on vastu võetud kooskõlas Euroopa õigusaktidega, eelkõige seoses isikuandmete kaitse, eraelu puutumatuse ja pettusevastase kaitsega.
Artiklis 29 viidatakse rahvusvahelisele koostööle, mida arendab digiülemineku ministeerium, eelkõige Euroopa Liidu tasandil.
Artiklis 30 viidatakse digiülemineku ministeeriumi pädevusele ENS5G rakendamisel. Ministeerium peaks koordineerima oma tegevust teiste küberturvalisuse ja elutähtsa taristu eest vastutavate asutustega, et tagada ENS5G järjepidev rakendamine.
Artiklis 31 on sätestatud ENS5G rakendamise volitused, mis vastavad digiülemineku ministeeriumile, sealhulgas näiteks ENS5G sisu väljatöötamine, täpsustamine ja üksikasjad, kehtestatud kohustuste täitmise kontrollimiseks ja kontrollimiseks tehtavate auditite läbiviimine ning riigiabi andmine.
Artikliga 32 antakse digiülemineku ministeeriumile kõik kontrollifunktsiooni volitused.
Karistussüsteemi käsitlevas artiklis 33 viidatakse 29. märtsi 2022. aasta kuningliku dekreetseaduse 7/2022 artiklitele 30 ja 31.
I lisas kirjeldatakse elemente, taristut ja ressursse, mis moodustavad 5G-võrgu.
II lisas on esitatud riigi tasandi riskianalüüs.
III lisas on sätestatud riskijuhtimine riigi tasandil.

9. Viienda põlvkonna ehk 5G mobiilside on uus elektroonilise side paradigma, millel on suur ümberkujundav potentsiaal ühiskonna ja majanduse hüvanguks, kuna avab võimaluse lisada uusi funktsioone, millel on suur mõju, nagu võrguandmetöötlus ja võimaldab luua virtuaalseid võrke, pakkudes madalat latentsusaega ja kõrge lisandväärtusega teenuseid sellistes valdkondades nagu meditsiin, transport ja energeetika.
Seetõttu edendavad nii Euroopa Liit kui ka Hispaania 5G-võrkude kiiret kasutuselevõttu ja 5G-teenuste osutamise kaudu nende kasulikkust eri sektorites.

5G-võrkudel ja -teenustel on eelmiste põlvkondadega võrreldes suhtelised turvaeelised. Siiski kujutavad need endast ka spetsiifilisi riske, mis tulenevad näiteks nende keerukamast, avatumast ja eristatud võrguarhitektuurist ning võimest transportida tohutul hulgal teavet ning võimaldada mitmete inimeste ja asjade samaaegset suhtlemist. Nende sidumine teiste võrkudega ja paljude ohtude piiriülene olemus mõjutavad nende turvalisust ning nende võrkude eeldatav laialdane kasutamine oluliste majanduslike ja ühiskondlike funktsioonide jaoks suurendab nende all kannatavate turvaintsidentide võimalikku mõju.
Neid 5G mobiilside uusi spetsiifilisi turvariske käsitleti regulatiivsetes aspektides kuninga 29. märtsi 2022. aasta dekreetseadusega 7/2022 viienda põlvkonna elektrooniliste sidevõrkude ja -teenuste turvalisuse tagamise nõuete kohta, mis hõlmab täielikult Euroopa Komisjoni 26. märtsi 2019. aasta soovitust (EL) 2019/534 5G-võrkude küberturvalisuse kohta, ning soovitusi, mille Euroopa Komisjon andis liikmesriikidele 29. jaanuari 2020. aasta teatisega 5G-võrkude turvalise kasutuselevõtu kohta ELis – ELi meetmepaketi rakendamine (COM/2020/50 final).
Eespool nimetatud 29. märtsi 2022. aasta kuningliku dekreetseadusega nr 7/2022 nähakse ette selle õiguslik areng 5G-võrkude ja -teenuste riikliku turvasüsteemi (ENS5G) kaudu.
Vastavalt eespool nimetatud kuningliku dekreetseaduse artikli 5 lõikele 3 käsitleb ENS5G põhjalikult 5G-võrkude ja -teenuste turvalisust, võttes arvesse panust 5G väärtusahela iga töötaja tegevusulatusse, samuti Euroopa Liidu, Rahvusvahelise Telekommunikatsiooni Liidu (ITU) ja teiste rahvusvaheliste organisatsioonide eeskirju, soovitusi ja tehnilisi standardeid, et tagada 5G-võrkude ja -teenuste turvaline kasutamine ja käitamine Hispaanias.
Kuninga dekreetseaduse artiklis 20 on omakorda sätestatud, et 5G-võrgu ja -teenuste jätkuva ja turvalise toimimise tagamiseks viib ENS5G läbi riigi tasandil riskianalüüsi 5G-võrkude ja teenuste turvalisuse kohta ning määrab kindlaks, täpsustab ja töötab välja meetmed analüüsitud riskide leevendamiseks ja juhtimiseks.
Lõpuks, kooskõlas kuningliku dekreetseaduse artikliga 21 kiidab valitsus pärast riikliku julgeolekunõukogu aruande saamist heaks ENS5G kuningliku dekreediga digiülemineku ministeeriumi ettepanekul.
Käesoleva määrusega kiidetakse heaks ENS5G, millega töötatakse välja 29. märtsi 2022. aasta kuningliku dekreetseaduse 7/2022 sätted viienda põlvkonna elektrooniliste sidevõrkude ja -teenuste turvalisuse tagamise nõuete kohta.

10. Eelnõuga otseselt seotud õigusaktid:

11. Ei

12.

13. Ei

14. Ei

15. Jah

16.
TBT aspekt: Ei

SPS aspekt: Ei

****
Euroopa Komisjon
Direktiivi (EL) 2015/1535 üldine kontaktinfo
e-post: grow-dir2015-1535-central@ec.europa.eu