Číslo oznámení : 2023/0761/ES (Spain)

# KRÁLOVSKÝ VÝNOS, KTERÝM SE SCHVALUJE NÁRODNÍ BEZPEČNOSTNÍ SYSTÉM PRO SÍTĚ A SLUŽBY 5G

Datum přijetí : 29/12/2023
Ukončení odkladné lhůty : 02/04/2024 (closed)

## Message

Zpráva 001

Zpráva od Komise - TRIS/(2023) 3739

Směrnice (EU) 2015/1535

Oznámení: 2023/0761/ES

Oznámení návrhu znění od členského státu

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.CS

1. MSG 001 IND 2023 0761 ES CS 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 - Telekomunikace

5. KRÁLOVSKÝ VÝNOS, KTERÝM SE SCHVALUJE NÁRODNÍ BEZPEČNOSTNÍ SYSTÉM PRO SÍTĚ A SLUŽBY 5G

6. Sítě a služby elektronických komunikací 5G

Telekomunikační zařízení.

7.

8. Nařízení se skládá z vysvětlující části, jediného článku, kterým se schvaluje Národní bezpečnostní systém pro sítě a služby 5G (ENS5G), dvou dodatečných ustanovení a 4 závěrečných ustanovení.
Nařízení o ENS5G, které má být schváleno, sestává z 33 článků rozdělených do osmi kapitol a tří příloh.
Důvodová zpráva vysvětluje důvody k přijetí nařízení a článků královského nařízení s mocí zákona, které jsou vypracovány.
V jediném článku se schvaluje Národní bezpečnostní systém pro sítě a služby 5G.
První dodatečné ustanovení stanoví, že vláda přezkoumává prostřednictvím královského výnosu na návrh Ministerstva digitální transformace a na základě zprávy Rady národní bezpečnosti národní bezpečnostní systém pro sítě a služby 5G, pokud to okolnosti vyžadují, a v každém případě každé čtyři roky.
Druhé dodatečné ustanovení stanoví, že královské nařízení s mocí zákona 7/2022 ze dne 29. března 2022 a ENS5G se budou vztahovat na generace elektronických komunikací následující po páté generaci, pokud pro ně neexistuje žádné zvláštní právní úprava.
První závěrečné ustanovení o názvu pravomoci uvádí, že královský výnos a systém, který schvaluje, jsou vydány na základě ustanovení čl. 149 odst. 1 bodu 21 a čl. 149 odst. 1 bodu 29 španělské ústavy, které svěřují státu výlučnou pravomoc v záležitostech obecného telekomunikačního systému a v záležitostech veřejné bezpečnosti.
V druhém závěrečném ustanovení se prohlašuje, že zákon č. 11/2022 ze dne 28. června 2022 o obecných telekomunikacích a jeho prováděcí nařízení jsou uplatňovány jako doplňkové, a uvádí, že ve všech záležitostech, které uvedené právní předpisy neupravují, se jako doplňující předpisy použijí královské nařízení s mocí zákona č. 12/2018 ze dne 7. září 2018 o bezpečnosti sítí a informačních systémů a zákon č. 8/2011 ze dne 28. dubna 2011, kterým se stanoví opatření na ochranu kritické infrastruktury, a jejich prováděcí nařízení.
Třetím závěrečným ustanovením o vývoji právních předpisů se umožňuje vedoucímu Ministerstva digitální transformace vypracovat ustanovení tohoto královského výnosu a systému, který schvaluje, a upravovat nařízením obsah příloh v souladu s vývojem technologického pokroku, schvalování nových technických norem a certifikačních systémů pro telekomunikační zařízení a spojené výrobky a vývoj různých konfigurací a technických parametrů sítí a služeb 5G a budoucích generací elektronických komunikací.
Ve čtvrtém závěrečném ustanovení se stanoví, že nařízení vstupuje v platnost prvním dnem po jeho zveřejnění v „Úředním státním věstníku“.
Pokud jde o obsah schváleného ENS5G:
V článku 1 se stanoví, že nařízení se vydává k provedení královského nařízení s mocí zákona 7/2022 ze dne 29. března 2022, zejména za použití kapitoly IV uvedeného nařízení.
V článku 2 se týká cílů nařízení, které již byly analyzovány.
V článku 3 se stanoví, že se použijí definice uvedené v královském nařízení s mocí zákona 7/2022 ze dne 29. března 2022, zákonu 11/2022 ze dne 28. června 2022 o obecných telekomunikacích a evropském kodexu pro elektronické komunikace.
V článku 4 se stanoví, že nařízení se vztahuje na provozovatele 5G, dodavatele 5G a podnikové uživatele 5G, kterým byla udělena práva používat veřejnou rádiovou doménu k instalaci, zavádění nebo provozování soukromé sítě 5G nebo k poskytování služeb 5G pro profesionální účely nebo k vlastní potřebě
V článku 5 se určují minimální prvky, infrastruktura a zdroje, které tvoří síť elektronických komunikací 5G, a odkazuje na jejich podrobný popis v příloze I. Stanoví rovněž kritické prvky sítě 5G, která musí být umístěna zpravidla na území státu (včetně možných výjimek).
Článek 6 se týká komplexního přístupu k bezpečnosti v souladu s mezinárodními právními předpisy Společenství a vnitrostátními právními předpisy, které byly schváleny nebo které mohou být schváleny, a požaduje, aby povinné strany provedly pomocí holistické metody analýzu zranitelnosti, hrozeb a rizik, které se jich jakožto hospodářských subjektů a různých složek dotýkají, jakož i přiměřené a komplexní řízení těchto rizik pomocí technik a opatření, které jsou vhodné k dosažení jejich zmírnění nebo odstranění a k dosažení konečného cíle bezpečného využívání a provozu sítí a služeb 5G.
V článku 7 se zdůrazňuje, že analýza a řízení rizik jsou nezbytnou součástí bezpečnostního procesu a musí představovat nepřetržitou a trvale aktualizovanou činnost.

Článek 8 se týká průběžného monitorování a pravidelného přehodnocování.
V článku 9 se stanoví, že analýza rizik na vnitrostátní úrovni je uvedena v příloze II a byla provedena s přihlédnutím k různým prvkům, jako jsou informace shromážděné od povinných stran, zkoumání zranitelnosti spojené s dodavatelským řetězcem sítí a služeb 5G, posouzení míry závislosti dodavatelů, riziko přerušení dodávek z důvodu hospodářských, podnikových nebo obchodních okolností ovlivňujících dodavatele nebo posouzení účinnosti použitých bezpečnostních opatření.
V článku 10 o řízení rizik na vnitrostátní úrovni se uvádí, že kritéria, požadavky, podmínky a časové lhůty stanovené pro povinné strany za účelem návrhu a provádění technik a opatření ke zmírnění rizika jsou stanoveny v příloze III.
Článek 11 rozvíjí ustanovení článku 14 královského nařízení s mocí zákona 7/2022 ze dne 29. března 2022, pokud jde o postup a aspekty, které má posoudit Rada ministrů ke klasifikaci dodavatelů jako vysoce rizikových, a prvků, které je třeba vzít v úvahu při objednávání případné výměny zařízení, výrobků a služeb poskytovaných těmito dodavateli. Stejně tak se v souladu s ustanoveními výše uvedeného královského nařízení s mocí zákona uvádí, že vysoce rizikoví poskytovatelé, jejichž telekomunikační zařízení, hardware, software nebo doplňkové služby jsou používány výhradně a výlučně v soukromých sítích 5G nebo k poskytování služeb 5G v rámci vlastního poskytování, jsou kvalifikováni jako dodavatelé se středním rizikem.
V článku 12 o určení lokalit, kde zařízení dodavatelů klasifikovaných jako vysoce rizikové nesmí být instalováno, se stanoví, že Národní bezpečnostní rada může na základě zprávy Ministerstva digitální transformace určit lokality, oblasti a centra, kde nesmí být instalováno zařízení dodavatelů klasifikovaných jako vysoce rizikoví. V případě instalace, úpravy nebo přizpůsobení rádiových stanic, které zajišťují pokrytí těchto lokalit, oblastí a center, musí provozovatelé 5G požádat Ministerstvo digitální transformace o povolení.
V článku 13 se ukládá provozovatelům sítí 5G povinnost navrhnout strategii diverzifikace dodavatelského řetězce a mít přenosová zařízení v přístupové síti, kterou poskytují alespoň dva různí dodavatelé. Stanoví rovněž kritéria, která má Rada ministrů zohlednit při rozhodování, zda je možné zachovat jediného dodavatele, pokud se v důsledku fúzí sníží počet dodavatelů. Kromě toho se uvádí předpoklady a postup, kterými může ministerstvo digitální transformace změnit strategii diverzifikace dodavatelského řetězce provozovatele 5G.
Článek 14 se zaměřuje na analýzu rizik, kterou mají provozovatelé 5G provést ve vztahu ke všem prvkům, infrastruktuře a zdrojům sítě uvedeným v příloze I, a uvádí faktory, které je třeba vzít v úvahu, a ukládá provozovatelům povinnost získat od svých dodavatelů bezpečnostní postupy a opatření přijatá v rámci produktů a služeb, které jim dodali, a zahrnout stanovení priorit a hierarchii rizik podle určitých parametrů, které jsou rovněž uvedeny. Provozovatelé sítí 5G musí analýzu rizik předložit do 1. října 2024 a poté každé 2 roky.
V článku 15 o analýze rizik ze strany dodavatelů 5G se vyžaduje analýza rizik telekomunikačních zařízení, hardwaru a softwaru a doplňkových služeb zapojených do fungování nebo provozu sítí 5G nebo poskytování služeb 5G a poskytnutí této analýzy ministerstvu na požádání. V případě dodavatelů klasifikovaných jako vysoce rizikoví nebo středně rizikoví se analýza předloží do 6 měsíců od této klasifikace a poté každé 2 roky.
V článku 16 o analýze rizik podnikovými uživateli 5G se vyžaduje, aby byla tato analýza rizik poskytnuta Ministerstvu pro digitální transformaci, jsou-li k tomu tito uživatelé povinni.
Článek 17 umožňuje Ministerstvu digitální transformace shromažďovat od povinných stran informace nezbytné pro analýzu rizik a neposkytnutí těchto informací do 15 pracovních dnů klasifikuje jako závažné porušení předpisů. Tyto informace jsou považovány za důvěrné a nelze je použít k jinému účelu, než je plnění cílů a povinností stanovených v královském nařízení s mocí zákona 7/2022 ze dne 29. března 2022, v ENS5G a v aktech vydaných k provedení obou ustanovení.
V článku 18 se prohlašuje, že řízení bezpečnostních rizik je obecnou povinností všech povinných stran.
Článek 19 se zaměřuje na řízení bezpečnosti ze strany provozovatelů 5G a uvádí povinnosti všech provozovatelů (např. přijímání pohotovostních plánů a opatření, dodržování evropských norem nebo technických specifikací a systémů certifikace, podrobit se na vlastní náklady bezpečnostnímu auditu nebo vyžadovat od svých dodavatelů, aby dodržovali bezpečnostní normy) a na další povinnosti pro ty provozovatele, kteří vlastní nebo provozují kritické prvky veřejné sítě 5G (např. zákaz používání zařízení od vysoce rizikových dodavatelů v kritických prvcích sítě nebo v určitých lokalitách, oblastech a centrech). Provozovatelé 5G musí popis technických a organizačních opatření navržených a prováděných za účelem řízení a zmírnění rizik předložit Ministerstvu pro digitální transformaci do 1. října 2024 a poté každé 2 roky. Kromě toho musí provozovatelé 5G, kteří vlastní nebo provozují kritické prvky veřejné sítě 5G, předložit Ministerstvu pro digitální transformaci strategii diverzifikace dodavatelského řetězce do 1. října 2024 a poté pokaždé, když je tato strategie předmětem změny. Informace o stavu provádění této strategie musí být předloženy do 1. října každého roku.

Článek 20 o řízení bezpečnosti ze strany dodavatelů 5G obsahuje seznam povinností, včetně provádění bezpečnostního auditu jejich zařízení, produktů a služeb, poskytování informací o možných zásazích třetích stran do návrhu, provozu a fungování jejich zařízení, produktů a služeb, a spolupráce s provozovateli sítí 5G a podnikovými uživateli 5G poskytováním informací a potvrzováním souladu s normami a certifikacemi. Dodavatelé 5G musí vypracovat zprávu ohledně technických a organizačních opatřeních navržených a prováděných za účelem řízení a zmírnění rizik a na požádání předložit tuto zprávu ministerstvu. V případě dodavatelů klasifikovaných jako vysoce rizikoví nebo středně rizikoví se zpráva předkládá do 6 měsíců od této klasifikace a poté každé 2 roky.
V článku 21 o řízení bezpečnosti podnikovými uživateli 5G se stanoví, že nesmějí používat v kritických prvcích sítě telekomunikační zařízení, přenosové systémy, přepínací nebo směrovací zařízení a jiné zdroje, které umožňují přenos signálů, hardwaru, softwaru nebo doplňkových služeb od dodavatelů, kteří byli klasifikováni jako středně rizikoví. Kromě toho musí uživatelé na požádání předložit Ministerstvu digitální transformace popis technických a organizačních opatření navržených a prováděných za účelem řízení a zmírnění rizik.
V článku 22 o řízení bezpečnosti orgány veřejné správy se stanoví, že z důvodů národní bezpečnosti nesmí orgány veřejné správy při instalaci, zavádění a provozu veřejných nebo soukromých sítí 5G nebo při poskytování služeb 5G, ať veřejně dostupných, nebo pro vlastní poskytování, používat zařízení, produkty a služby poskytované vysoce rizikovými nebo středně rizikovými dodavateli.
V článku 23 se stanoví, že v souladu s povinnostmi stanovenými v předchozích článcích berou povinné strany v úvahu a uplatňují ustanovení stanovená královským nařízením s mocí zákona 7/2022 ze dne 29. března 2022, v ENS5G a v aktech, které jsou vydány k provedení obou ustanovení.
Článkem 24 se umožňuje Ministerstvu digitální transformace shromažďovat od povinných stran informace nezbytné pro řízení rizik a neposkytnutí těchto informací do 15 pracovních dnů klasifikuje jako závažné porušení předpisů. Tyto informace jsou považovány za důvěrné a nelze je použít k jinému účelu, než je plnění cílů a povinností stanovených v královském nařízení s mocí zákona 7/2022 ze dne 29. března 2022, v ENS5G a v aktech vydaných k provedení obou ustanovení.
V článku 25 se stanoví, že všechny povinné strany, jakož i orgány veřejné správy, výrobci, dovozci, distributoři a ti, kteří uvádějí na trh a prodávají koncová zařízení a zařízení s cílem připojení k síti 5G a aby mohli poskytovat služby 5G, musí spolupracovat a předložit informace požadované pro úpravu a provádění ENS5G.
V článku 26 se stanoví, že nařízením vedoucího Ministerstva digitální transformace může být použití určitého zařízení, systému, programu nebo služby podmíněno předchozí certifikací podle nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o kybernetické bezpečnosti nebo v rámci systémů certifikace a technických norem pro certifikaci zařízení a výrobků 5G, které mohou být schváleny na evropské nebo mezinárodní úrovni.
V článku 27 se stanoví, že nařízení se použije, aniž jsou dotčeny právní předpisy v oblasti zahraničních investic a hospodářské soutěže.
V článku 28 o koncových zařízeních se stanoví, že výroba, dovoz, distribuce, uvádění na trh a prodej koncových zařízení a zařízení pro připojení k síti 5G a pro poskytování služeb 5G jsou podmíněny dodržováním bezpečnostních požadavků na digitální produkty a platných základních požadavků týkajících se kybernetické bezpečnosti přijatých v souladu s evropskými právními předpisy, zejména pokud jde o ochranu osobních údajů, soukromí a ochranu před podvody.
Článek 29 se týká mezinárodní spolupráce, kterou má rozvíjet Ministerstvo digitální transformace, zejména na úrovni Evropské unie.
Článek 30 se týká pravomoci Ministerstva digitální transformace pro provádění ENS5G. Ministerstvo by mělo koordinovat činnost s ostatními subjekty odpovědnými za kybernetickou bezpečnost a kritickou infrastrukturu, aby bylo zajištěno důsledné provádění ENS5G.
V článku 31 se rozdělují pravomoci pro provádění ENS5G, které odpovídají Ministerstvu digitální transformace, včetně například vývoje, specifikace a podrobností obsahu ENS5G, provádění auditů za účelem ověření a kontroly dodržování uložených povinností a poskytování veřejné podpory.
V článku 32 se připisují Ministerstvu digitální transformace veškeré pravomoci kontrolní funkce.
V článku 33 o systému sankcí se odkazuje na ustanovení článků 30 a 31 královského nařízení s mocí zákona 7/2022 ze dne 29. března 2022.
Příloha I popisuje prvky, infrastrukturu a zdroje, které tvoří síť 5G.
Příloha II obsahuje analýzu rizik na vnitrostátní úrovni.
Příloha III stanoví řízení rizik na vnitrostátní úrovni.

9. Mobilní komunikace páté generace neboli 5G představují nové paradigma elektronických komunikací s velkým transformačním potenciálem ve prospěch společnosti a ekonomiky, neboť otevírají možnost začlenění nových funkcí, které budou mít velký dopad, jako je síťová výpočetní technika, a umožňují vytváření virtuálních sítí, které nabízejí nízkou latenci a poskytují služby s vysokou přidanou hodnotou v oblastech, jako je medicína, doprava a energetika.
Evropská unie i Španělsko proto podporují rychlé zavádění sítí 5G a provádění projektů prokazujících jejich užitečnost pro různá odvětví prostřednictvím poskytování služeb 5G.
Sítě a služby 5G mají oproti předchozím generacím poměrné bezpečnostní výhody. Představují však také specifická rizika, která vyplývají například z jejich složitější, otevřenější a nejednotné síťové architektury a z jejich schopnosti přenášet obrovské objemy informací a umožňovat souběžnou interakci více lidí a věcí. Jejich propojení s jinými sítěmi a nadnárodní povaha mnoha hrozeb mají dopad na jejich bezpečnost a předvídatelné rozsáhlé využívání těchto sítí pro základní hospodářské a společenské funkce zvýší potenciální dopad bezpečnostních incidentů, kterými trpí.
Tato nová specifická bezpečnostní rizika mobilních komunikací 5G byla řešena z regulačního hlediska prostřednictvím královského legislativního nařízení 7/2022 ze dne 29. března 2022 o požadavcích na zajištění bezpečnosti sítí a služeb elektronických komunikací páté generace, které plně zahrnuje doporučení Evropské komise (EU) 2019/534 ze dne 26. března 2019 Kybernetická bezpečnost sítí 5G, jakož i doporučení, která byla členským státům poskytnuta s ohledem na používání tohoto souboru nástrojů ve sdělení Evropské komise ze dne 29. ledna 2020 o bezpečném zavádění sítí 5G v EU – implementace souboru nástrojů EU (COM/2020/50 final).
Výše uvedené královské nařízení s mocí zákona 7/2022 ze dne 29. března 2022 stanoví jeho regulační vývoj prostřednictvím národního bezpečnostního systému pro sítě a služby 5G (ENS5G).
V souladu s čl. 5 odst. 3 výše uvedeného královského nařízení s mocí zákona provede ENS5G komplexní úpravu bezpečnosti sítí a služeb 5G s přihlédnutím k přínosu každého zástupce hodnotového řetězce 5G, jakož i k předpisům, doporučením a technickým normám Evropské unie, Mezinárodní telekomunikační unie (ITU) a dalším mezinárodním organizacím, aby byl zaručen konečný cíl bezpečného využívání a provozu sítí a služeb 5G ve Španělsku.
Článek 20 královského nařízení s mocí zákona stanoví, že za účelem zajištění nepřetržitého a bezpečného fungování sítě a služeb 5G provede ENS5G na vnitrostátní úrovni analýzu rizik týkajících se bezpečnosti sítí a služeb 5G a určí, specifikuje a vypracuje opatření ke zmírnění a řízení analyzovaných rizik.
Závěrem, v souladu s článkem 21 královského nařízení s mocí zákona, bude ENS5G schválen vládou, královským výnosem na návrh Ministerstva digitální transformace podaný na základě zprávy Národní bezpečnostní rady.
Tímto nařízením se schvaluje ENS5G a rozvíjí ustanovení královského nařízení s mocí zákona 7/2022 ze dne 29. března 2022 o požadavcích na zajištění bezpečnosti sítí a služeb elektronických komunikací páté generace.

10. Odkazy na základní texty:

11. Ne

12.

13. Ne

14. Ne

15. Ano

16.
Hledisko TBT: Ne

Hledisko SPS: Ne

**********
Evropská komise
Kontaktní bod směrnice (EU) 2015/1535
email: grow-dir2015-1535-central@ec.europa.eu