



EUROPEAN COMMISSION

Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs

Single Market Enforcement

Notification of Regulatory Barriers

Broj notifikacije : 2023/0761/ES (Spain)

KRALJEVSKA UREDBA O ODOBRENJU NACIONALNOG PROGRAMA SIGURNOSTI ZA 5G MREŽE I USLUGE

Datum zaprimanja : 29/12/2023

Prestanak razdoblja mirovanja : 02/04/2024 (closed)

Message

Poruka 001

Priopćenje Komisijev- TRIS/(2023) 3739

Direktiva (EU) 2015/1535

Obavijest: 2023/0761/ES

Obavijest o nacrtu teksta iz države članice

Notification – Notificación – Notifizierung – 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 - Καμία έναρξη προθεσμίας - No abre el plazo - Viivituste perioodi ei avata - Määräaika ei ala tästä - Ne otvara razdoblje kašnjenja - Nem nyitja meg a késéset - Non fa decorrere la mora - Atidējimai nepradedami - Atlikšanas laikposms nesākas - Ma jiftaħ 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.HR

1. MSG 001 IND 2023 0761 ES HR 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 - Telekomunikacije

5. KRALJEVSKA UREDBA O ODOBRENJU NACIONALNOG PROGRAMA SIGURNOSTI ZA 5G MREŽE I USLUGE

6. 5G elektroničke komunikacijske mreže i usluge



EUROPEAN COMMISSION

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

Telekomunikacijska oprema.

7.

8. Propis se sastoji od dijela s objašnjenjima, jednog članka kojim se odobrava program ENS5G (Nacionalni program sigurnosti za 5G), dvije dodatne odredbe i četiri završne odredbe.

Program ENS5G koji se odobrava sastoji se od 33 članka podijeljena u osam poglavlja i tri priloga.

U obrazloženju se objašnjavaju razlozi za donošenje propisa i navode članci Kraljevske uredbe sa zakonskom snagom koji se izrađuju.

Jedinim člankom odobrava se Nacionalni program sigurnosti za 5G mreže i usluge.

U prvoj dodatnoj odredbi navodi se da vlada u skladu s Kraljevskom uredbom, na prijedlog Ministarstva digitalne transformacije, nakon izvješća Vijeća za nacionalnu sigurnost, preispituje Nacionalni program sigurnosti za 5G mreže i usluge kada to okolnosti zahtijevaju, a u svakom slučaju svake četiri godine.

U drugoj dodatnoj odredbi navodi se da se Kraljevska uredba sa zakonskom snagom 7/2022 od 29. ožujka 2022. i program ENS5G primjenjuju na generacije elektroničkih komunikacija nakon pete generacije, dok za njih ne postoji poseban propis.

U prvoj završnoj odredbi o pravu nadležnosti navodi se da su Kraljevska uredba i program koji se njome odobrava izdani na temelju odredbi članka 149. stavka 1. točke 21. i članka 149. stavka 1. točke 29. španjolskog Ustava, kojima se državi dodjeljuje isključiva nadležnost u pogledu općeg telekomunikacijskog sustava i u pitanjima javne sigurnosti.

Drugom završnom odredbom propisuje se dodatna primjena Zakona 11/2022 od 28. lipnja 2022. o općim telekomunikacijama i njegovih provedbenih propisa te se navodi da se u svim pitanjima koja nisu uređena tim zakonodavstvom dodatno primjenjuju Kraljevska uredba sa zakonskom snagom 12/2018 od 7. rujna 2018. o sigurnosti mrežnih i informacijskih sustava i Zakon 8/2011 od 28. travnja 2011. o uspostavi mjera za zaštitu kritične infrastrukture, kao i njihovi provedbeni propisi.

Treća završna odredba o regulatornom razvoju omogućuje nadležnoj osobi u Ministarstvu za digitalnu transformaciju da razvije odredbe ove Kraljevske uredbe i program koji odobrava te da odlukom izmijeni sadržaj priloga u skladu s razvojem tehnološkog napretka, odobravanjem novih tehničkih normi i programa certificiranja za telekomunikacijsku opremu i povezane proizvode te razvojem različitih konfiguracija i tehničkih parametara 5G mreža i usluga te budućih generacija elektroničkih komunikacija.

Četvrtom završnom odredbom predviđeno je da propis stupi na snagu sljedećeg dana od dana objave u „Službenom listu”.

U pogledu sadržaja programa ENS5G koji se odobrava:

U članku 1. navodi se da se propis donosi u okviru provedbe Kraljevske uredbe sa zakonskom snagom 7/2022 od 29. ožujka 2022., osobito primjenom njezina poglavlja IV.

Članak 2. odnosi se na ciljeve propisa koji su već analizirani.

U članku 3. navodi se da se upotrebljavaju definicije utvrđene u Kraljevskoj uredbi sa zakonskom snagom 7/2022 od 29. ožujka 2022., Zakonu 11/2022 od 28. lipnja 2022. o općim telekomunikacijama i Europskom zakoniku elektroničkih komunikacija.

Člankom 4. predviđa se da se propis primjenjuje na operatore 5G tehnologije, dobavljače 5G tehnologije i poslovne korisnike 5G tehnologije koji imaju pravo na uporabu javne radijske domene za ugradnju, uvođenje ili rad privatne 5G mreže ili za pružanje 5G usluga u profesionalne ili vlastite svrhe.

U članku 5. utvrđuju se minimalni elementi, infrastruktura i resursi koji čine 5G elektroničku komunikacijsku mrežu, pri čemu se upućuje na Prilog I. za njihov detaljan opis. Tim se člankom utvrđuju i ključni elementi 5G mreže koji se u pravilu moraju nalaziti na državnom području (uključujući moguće iznimke).

Članak 6. odnosi se na sveobuhvatni pristup sigurnosti u skladu s međunarodnom zajednicom i nacionalnim zakonodavstvom koje je odobreno ili koje se može odobriti, a kojim se od stranaka obveznica zahtijeva da sveobuhvatnom metodom provedu analizu ranjivosti, prijetnji i rizika koji utječu na njih kao gospodarske subjekte i različitih komponenti, kao i primjereno i sveobuhvatno upravljanje tim rizicima primjenom tehnika i mjera koje su prikladne za postizanje njihova ublažavanja ili uklanjanja te za postizanje krajnjeg cilja sigurne uporabe i rada 5G mreža i usluga.

U članku 7. naglašava se da su analiza rizika i upravljanje rizikom ključan dio sigurnosnog procesa i da bi trebali biti



EUROPEAN COMMISSION

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

stalna aktivnost koja se kontinuirano ažurira.

Članak 8. odnosi se na kontinuirano praćenje i periodično ponovno ocjenjivanje.

U članku 9. navodi se da analiza rizika na nacionalnoj razini odgovara onoj utvrđenoj u Prilogu II. i da je provedena uzimajući u obzir različite elemente kao što su informacije prikupljene od stranaka obveznica, ispitivanje ranjivosti povezanih s lancem opskrbe 5G mrežama i uslugama, procjena stupnja ovisnosti dobavljača, rizik od prekida opskrbe zbog gospodarskih, korporativnih ili komercijalnih okolnosti koje utječu na dobavljače ili procjena učinkovitosti primijenjenih sigurnosnih mjera.

U članku 10. o upravljanju rizicima na nacionalnoj razini navodi se da su kriteriji, zahtjevi, uvjeti i rokovi u kojima stranke obveznice osmišljavaju i provode tehnike i mjere za smanjenje rizika utvrđeni u Prilogu III.

Člankom 11. razrađuju se odredbe članka 14. Kraljevske uredbe sa zakonskom snagom 7/2022 od 29. ožujka 2022. u pogledu postupka i aspekata koje Vijeće ministara treba ocijeniti za kvalifikaciju dobavljača kao visokorizičnih i elemenata koje treba uzeti u obzir prilikom zahtijevanja moguće zamjene opreme, proizvoda i usluga koje pružaju ti dobavljači. Isto tako, u skladu s odredbama prethodno navedene Kraljevske uredbe sa zakonskom snagom, navodi se da visokorizični dobavljači čija se telekomunikacijska oprema, hardver, softver ili pomoćne usluge upotrebljavaju samo i isključivo u privatnim 5G mrežama ili za pružanje 5G usluga za vlastite potrebe smatraju srednjerizičnim dobavljačima.

U članku 12. o utvrđivanju lokacija na kojima se oprema dobavljača koji su klasificirani kao visokorizičnih ne smije ugraditi navodi se da Vijeće za nacionalnu sigurnost, nakon izvješća Ministarstva digitalne transformacije, može utvrditi lokacije, područja i centre na kojima se ne smije ugraditi oprema dobavljača klasificiranih kao visokorizični dobavljači. Za ugradnju, izmjenu ili prilagodbu radijskih postaja kojima se osigurava pokrivenost tih lokacija, područja i centara operatori 5G tehnologije moraju zatražiti odobrenje Ministarstva za digitalnu transformaciju.

U skladu s člankom 13. operatori 5G tehnologije obvezni su osmisлити strategiju diversifikacije opskrbnog lanca i imati prijenosnu opremu u pristupnoj mreži koju pružaju najmanje dva različita dobavljača. Tim se člankom također predviđaju kriteriji koje Vijeće ministara treba uzeti u obzir kako bi odlučilo je li moguće zadržati jednog dobavljača ako je broj dobavljača smanjen zbog spajanja. Osim toga, navode se pretpostavke i postupak na temelju kojih Ministarstvo za digitalnu transformaciju može izmijeniti strategiju diversifikacije opskrbnog lanca operatora 5G tehnologije.

Članak 14. usmjeren je na analizu rizika koju trebaju provesti operatori 5G tehnologije u odnosu na sve elemente, infrastrukturu i resurse mreže u Prilogu I. U njemu se također navode čimbenici koje treba uzeti u obzir te se obavezuje operatore da od svojih dobavljača prikupljaju sigurnosne prakse i mjere donesene u proizvodima i uslugama koje su im isporučili te da uključe određivanje prioriteta i hijerarhiju rizika u skladu s određenim parametrima koji su također navedeni. Operatori 5G tehnologije moraju dostaviti analizu rizika do 1. listopada 2024., a nakon toga svake dvije godine.

Člankom 15. o analizi rizika dobavljača 5G tehnologije zahtijeva se analiza rizika telekomunikacijske opreme, hardvera i softvera te pomoćnih usluga uključenih u funkcioniranje ili rad 5G mreža ili pružanje 5G usluga te pružanje navedene analize Ministarstvu na zahtjev. U slučaju dobavljača koji su klasificirani kao visokorizični ili srednjerizični, analiza se dostavlja u roku od šest mjeseci od te klasifikacije i svake dvije godine nakon toga.

Člankom 16. o analizi rizika korporativnih korisnika 5G tehnologije zahtijeva se da se ta analiza rizika dostavi Ministarstvu digitalne transformacije ako su takvi korisnici obvezni to učiniti.

Člankom 17. Ministarstvu digitalne transformacije omogućuje se da od stranaka obveznica prikupi informacije potrebne za analizu rizika, a nepružanje takvih informacija u roku od 15 radnih dana klasificira se kao teška povreda. Informacije se smatraju povjerljivima i ne smiju se upotrebljavati u drugu svrhu osim ispunjenja ciljeva i obveza utvrđenih Kraljevskom uredbom sa zakonskom snagom 7/2022 od 29. ožujka 2022., programa ENS5G-om i aktima koji se izdaju u okviru provedbe obaju propisa.

Člankom 18. utvrđuje se opća dužnost svih stranaka obveznica da upravljaju sigurnosnim rizicima.

Članak 19. usmjeren je na upravljanje sigurnošću putem operatora 5G tehnologije, uz navođenje obveza za sve operatore (kao što su donošenje kriznih planova i mjera, usklađivanje s europskim normama ili tehničkim specifikacijama i programima certificiranja, podvrgavanje sigurnosnoj reviziji na vlastiti trošak ili zahtijevanje od njihovih dobavljača da poštuju sigurnosne standarde) i dodatne obveze za operatore koji posjeduju ključne elemente javne 5G mreže ili upravljaju njome (kao što su zabrane uporabe opreme visokorizičnih dobavljača u kritičnim mrežnim elementima ili na određenim lokacijama, područjima i centrima). Operatori 5G tehnologije moraju Ministarstvu digitalne transformacije dostaviti opis tehničkih i organizacijskih mjera osmišljenih i provedenih radi upravljanja rizicima i njihova ublažavanja do 1. listopada 2024. i svake dvije godine nakon toga. Osim toga, operatori 5G tehnologije koji posjeduju ključne elemente javne 5G mreže ili upravljaju njima moraju Ministarstvu za digitalnu transformaciju dostaviti strategiju diversifikacije opskrbnog lanca do 1. listopada 2024. i nakon toga svaki put kada je podložna izmjenama. Informacije o stanju provedbe



EUROPEAN COMMISSION

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

te strategije moraju se dostaviti do 1. listopada svake godine.

Članak 20. o upravljanju sigurnošću putem dobavljača 5G tehnologije sadržava popis obveza, uključujući provedbu sigurnosne revizije njihove opreme, proizvoda i usluga, pružanje informacija o mogućim smetnjama trećih strana u projektiranju, radu i funkcioniranju njihove opreme, proizvoda i usluga te suradnju s operatorima 5G tehnologije i korporativnim korisnicima 5G tehnologije kroz pružanje informacija i potvrđivanje sukladnosti s normama i certifikatima. Dobavljači 5G tehnologije moraju pripremiti izvješće o tehničkim i organizacijskim mjerama koje su osmišljene i provedene za upravljanje rizicima i njihovo ublažavanje te na zahtjev dostaviti navedeno izvješće Ministarstvu. U slučaju dobavljača koji su klasificirani kao visokorizični ili srednjerizični, izvješće se dostavlja u roku od šest mjeseci od te klasifikacije i svake dvije godine nakon toga.

U članku 21. o upravljanju sigurnošću putem korporativnih korisnika 5G tehnologije navodi se da oni ne smiju u ključnim mrežnim elementima upotrebljavati telekomunikacijsku opremu, sustave prijenosa, opremu za komutiranje ili usmjeravanje i druga sredstva koja omogućuju prijenos signala, hardvera, softvera ili pomoćnih usluga dobavljača koji su klasificirani kao visokorizični. Osim toga, korisnici moraju Ministarstvu gospodarstva i digitalne transformacije na zahtjev dostaviti opis tehničkih i organizacijskih mjera osmišljenih i provedenih za upravljanje rizicima i njihovo ublažavanje.

U članku 22. o upravljanju sigurnošću putem javnih uprava navodi se da, zbog razloga nacionalne sigurnosti, pri ugradnji, uvođenju i radu 5G mreža, bilo javnih ili privatnih, ili pružanju 5G usluga, bilo da su javno dostupne ili za vlastite potrebe, javne uprave ne smiju upotrebljavati opremu, proizvode i usluge koje pružaju visokorizični ili srednjerizični dobavljači.

U članku 23. navodi se da, u skladu s obvezama iz prethodnih članaka, stranke obveznice uzimaju u obzir i primjenjuju ono što je utvrđeno Kraljevskom uredbom sa zakonskom snagom 7/2022 od 29. ožujka 2022., programom ENS5G i aktima koji se izdaju u okviru provedbe obaju propisa.

Člankom 24. Ministarstvu digitalne transformacije omogućuje se da od stranaka obveznica prikupi informacije potrebne za upravljanje rizicima, a nepružanje takvih informacija u roku od 15 radnih dana klasificira se kao teška povreda.

Informacije se smatraju povjerljivima i ne smiju se upotrebljavati u drugu svrhu osim ispunjenja ciljeva i obveza utvrđenih Kraljevskom uredbom sa zakonskom snagom 7/2022 od 29. ožujka 2022., programa ENS5G-om i aktima koji se izdaju u okviru provedbe obaju propisa.

U članku 25. navodi se da sve stranke obveznice, kao i javne uprave, proizvođači, uvoznici, distributeri i oni koji stavljaju na tržište i prodaju terminalnu opremu i uređaje za povezivanje na 5G mrežu te za pružanje 5G usluga moraju surađivati i dostaviti informacije potrebne za izmjenu i provedbu programa ENS5G.

U članku 26. navodi se da se odlukom nadležne osobe Ministarstva za digitalnu transformaciju uporaba određenog dijela opreme, sustava, programa ili usluge može uvjetovati prethodnom certifikacijom na temelju Uredbe (EU) 2019/881 Europskog parlamenta i Vijeća od 17. travnja 2019. o kibersigurnosti ili u okviru programa certifikacije i tehničkih normi za certifikaciju 5G opreme i proizvoda koji se mogu odobriti na europskoj ili međunarodnoj razini.

U članku 27. navodi se da se propis primjenjuje ne dovodeći u pitanje strana ulaganja i pravo tržišnog natjecanja.

Člankom 28. o terminalnoj opremi predviđeno je da proizvodnja, uvoz, distribucija, stavljanje na tržište i prodaja terminalne opreme i uređaja za povezivanje na 5G mrežu i pružanje 5G usluga ovise o usklađenosti sa sigurnosnim zahtjevima za digitalne proizvode i primjenjivim bitnim zahtjevima u pogledu kibersigurnosti donesenima u skladu s europskim zakonodavstvom, posebno u pogledu zaštite osobnih podataka, privatnosti i zaštite od prijevара.

Članak 29. odnosi se na međunarodnu suradnju koju treba razviti Ministarstvo digitalne transformacije, posebno na razini Europske unije.

Članak 30. odnosi se na nadležnost Ministarstva digitalne transformacije za provedbu programa ENS5G. Ministarstvo bi se trebalo koordinirati s drugim tijelima nadležnima za kibersigurnost i ključnu infrastrukturu kako bi se osigurala dosljedna provedba programa ENS5G.

U članku 31. utvrđuju se ovlasti za provedbu programa ENS5G koje se dodjeljuju Ministarstvu digitalne transformacije, uključujući, na primjer, razvoj, specifikaciju i detalje sadržaja programa ENS5G, provedbu revizija radi provjere i praćenja usklađenosti s propisanim obvezama te dodjelu javne potpore.

Člankom 32. Ministarstvu digitalne transformacije dodjeljuju se sve ovlasti funkcije inspekcijskih pregleda.

Članak 33. o sustavu kazni odnosi se na odredbe članaka 30. i 31. Kraljevske uredbe sa zakonskom snagom 7/2022 od 29. ožujka 2022.

U Prilogu I. opisani su elementi, infrastruktura i resursi koji čine 5G mrežu.

Prilog II. sadržava analizu rizika na nacionalnoj razini.

U Prilogu III. utvrđeno je upravljanje rizicima na nacionalnoj razini.



EUROPEAN COMMISSION

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

9. Mobilne komunikacije pete generacije ili 5G mobilne komunikacije nova su paradigma elektroničkih komunikacija s velikim transformativnim potencijalom za dobrobit društva i gospodarstva jer otvaraju mogućnost uključivanja novih funkcionalnosti koje će imati velik učinak kao što su mrežno računalstvo i omogućuju stvaranje virtualnih mreža, pružaju nisku latenciju te usluge s visokom dodanom vrijednošću u područjima kao što su medicina, promet i energetika. Stoga i Europska unija i Španjolska promiču brzo uvođenje 5G mreža i provedbu projekata kojima se dokazuje njihova korisnost za različite sektore pružanjem 5G usluga.

5G mreže i usluge imaju komparativne sigurnosne prednosti u odnosu na prethodne generacije. Međutim, one također predstavljaju posebne rizike koji proizlaze, na primjer, iz složenije, otvorenije i raščlanjene mrežne arhitekture, kao i iz njihove sposobnosti prijenosa golemih količina informacija i omogućavanja istodobne interakcije više ljudi i stvari. Njihova međusobna povezanost s drugim mrežama i transnacionalna priroda mnogih prijetnji utječu na njihovu sigurnost, a predvidljiva raširena upotreba tih mreža za osnovne gospodarske i društvene funkcije povećat će mogući učinak sigurnosnih incidenata kojima su izložene.

Ti novi posebni sigurnosni rizici 5G mobilnih komunikacija riješeni su u regulatornom smislu Kraljevskom uredbom sa zakonskom snagom 7/2022 od 29. ožujka 2022. o zahtjevima za osiguranje sigurnosti pete generacije elektroničkih komunikacijskih mreža i usluga koja u potpunosti uključuje Preporuku Europske komisije (EU) 2019/534 od 26. ožujka 2019. o kibersigurnosti 5G mreža, kao i preporuke koje su u Komunikaciji Europske komisije od 29. siječnja 2020. o sigurnom uvođenju 5G mreža u EU-u — Provedba paketa instrumenata EU-a (COM/2020/50 final) državama članicama pružene u pogledu upotrebe tog paketa instrumenata.

Navedenom Kraljevskom uredbom sa zakonskom snagom 7/2022 od 29. ožujka 2022. predviđa se njezin regulatorni razvoj putem Nacionalnog programa sigurnosti za 5G mreže i usluge (ENS5G).

U skladu s člankom 5. stavkom 3. spomenute Kraljevske uredbe sa zakonskom snagom, programom ENS5G provodi se sveobuhvatan pristup sigurnosti 5G mreža i usluga, uzimajući u obzir doprinose opsegu svakog agenta u 5G vrijednosnom lancu, kao i propise, preporuke i tehničke norme Europske unije, Međunarodne telekomunikacijske unije (ITU) i drugih međunarodnih organizacija, kako bi se zajamčio krajnji cilj sigurnog korištenja i upravljanja 5G mrežama i uslugama u Španjolskoj.

S druge strane, člankom 20. Kraljevske uredbe sa zakonskom snagom predviđeno je da se kroz program ENS5G na nacionalnoj razini provodi analiza rizika u pogledu sigurnosti 5G mreža i usluga te utvrđuju, određuju i razvijaju mjere za ublažavanje analiziranih rizika i upravljanje njima kako bi se osiguralo trajno i sigurno funkcioniranje 5G mreže i usluga. Naposljetku, u skladu s člankom 21. Kraljevske uredbe sa zakonskom snagom, program ENS5G odobrava vlada u skladu s Kraljevskom uredbom, na prijedlog Ministarstva digitalne transformacije te nakon izvješća Vijeća za nacionalnu sigurnost. Ovom se Uredbom odobrava program ENS5G kojim se razvijaju odredbe Kraljevske uredbe sa zakonskom snagom 7/2022 od 29. ožujka 2022. o zahtjevima za osiguranje sigurnosti pete generacije elektroničkih komunikacijskih mreža i usluga.

10. Upućivanja na temeljne tekstove:

11. Ne

12.

13. Ne

14. Ne

15. Da

16.

Sa stajališta TBT-a: Ne

Sa stajališta SPS-a: Ne

Europska komisija



EUROPEAN COMMISSION

Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs

Single Market Enforcement

Notification of Regulatory Barriers

Služba za kontakt Direktive (EU) 2015/1535

E-pošta: grow-dir2015-1535-central@ec.europa.eu