



EUROPEAN COMMISSION

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

Notifikationsnummer : 2026/0346/ES (Spain)

Udkast til kongeligt dekret om sikkerhed og modstandsdygtighed i elektroniske kommunikationsnet og -tjenester og visse digitale infrastrukturer

Modtagelsesdato : 08/07/2026

Afslutning af status quo-periode : 09/10/2026

Message

Meddelelse 001

Kommissionens meddelelse - TRIS/(2026) 1822

Direktiv (EU) 2015/1535

Notifikation: 2026/0346/ES

Notifikation af et udkast fra en medlemsstat

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 - Καμμία 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: 20261822.DA

1. MSG 001 IND 2026 0346 ES DA 08-07-2026 ES NOTIF

2. Spain

3A. Subdirección General de Ordenación de las Telecomunicaciones.

Secretaría General de Telecomunicaciones, Infraestructuras Digitales y Seguridad Digital.

Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales.

Ministerio para la Transformación Digital y de la Función Pública

Calle Poeta Joan Maragall 41

28020 Madrid

+34 913462750

3B. Subdirección General de Ordenación de las Telecomunicaciones.

Secretaría General de Telecomunicaciones, Infraestructuras Digitales y Seguridad Digital.

Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales.

Ministerio para la Transformación Digital y de la Función Pública



EUROPEAN COMMISSION

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

Calle Poeta Joan Maragall 41
28020 Madrid
+34 913462750

4. 2026/0346/ES - V00T - Teletjenester

5. Udkast til kongeligt dekret om sikkerhed og modstandsdygtighed i elektroniske kommunikationsnet og -tjenester og visse digitale infrastrukturer

6. Formålet er at styrke sikkerheden, modstandsdygtigheden og kontinuiteten i elektroniske kommunikationsnet og -tjenester, deres tilhørende faciliteter og visse digitale infrastrukturer i Spanien.

7.

8. Det kongelige dekret har til formål at skabe sikkerhed, modstandsdygtighed og kontinuitet i elektroniske kommunikationsnet og -tjenester, deres tilhørende faciliteter og visse digitale infrastrukturer i Spanien.

Formålet er, at væsentlige tjenester fortsat leveres i tilfælde af sikkerhedshændelser, driftsforstyrrelser eller markante forringelser af tjenesternes kvalitet, samt at fastlægge forpligtelserne til at indberette sådanne hændelser til myndighederne.

De forpligtede enheder er operatører af offentlige elektroniske kommunikationsnet, udbydere af offentligt tilgængelige tjenester, operatører af tilknyttede anlæg og digital infrastruktur såsom undersøiske kabler, satellitsystemer, databehandlingscentre (DPC'er), indholdsleveringsnetværk (CDN'er) og internetudvekslingspunkter (IXP'er) samt, i visse henseender, 112-alarmcentraler og offentlige varslingssystemer. Dekretet understreger også, at disse netværk og infrastrukturer spiller en afgørende rolle i nødsituationer.

Der er udarbejdet en "Plan for national sikkerhed og modstandsdygtighed", som skal fastlægge, hvordan kriseindsatsen skal organiseres, samt de institutionelle koordineringsmekanismer. Den fastsætter desuden, at de forpligtede enheder skal udarbejde en "generel plan" for hver forpligtet part samt "specifikke planer" for hver netværkstype og for specifikke tjenester. De skal omfatte risikoanalyser, identifikation af kritisk infrastruktur, forebyggende foranstaltninger, genopretningsmekanismer og handlingsplaner for forskellige scenarier, såsom strømafbrydelser, naturkatastrofer, brande, it-nedbrud eller cyberangreb.

Der indføres særlige forpligtelser for at sikre kontinuiteten i telekommunikationstjenesterne. Operatørerne skal træffe foranstaltninger for at minimere konsekvenserne af hændelser og sikre, at væsentlige tjenester, især nødkommunikation, fungerer. Under ekstraordinære omstændigheder kan de prioritere visse typer trafik, f.eks. nødkommunikation eller tale- og SMS-tjenester, samtidig med at de altid respekterer princippet om teknologineutralitet. Derudover fastsættes der mindstekrav til energiuafhængighed for kritisk infrastruktur, og mobilnetværkene pålægges en forpligtelse til gradvist inden for tre år at sikre mindst fire timers reservestrøm til 75 % af befolkningen.

Det omfatter et system til indberetning af væsentlige hændelser, der ikke betragtes som cybersikkerhedshændelser, idet disse er reguleret i NIS2-direktivet og CER-direktivet. Operatørerne skal underrette statssekretariatet om enhver væsentlig hændelse senest én time efter, at de er blevet opmærksomme på den, og skal derefter regelmæssigt fremsende opdateringer, så længe forstyrrelsen varer, efterfulgt af en afsluttende rapport, når tjenesten er genoprettet. Der fastsættes specifikke foranstaltninger for nødopkald via nummeret 112 og offentlige varslingssystemer. Både alarmcentraler og operatører skal indføre redundans- og driftskontinuitetsforanstaltninger, udarbejde specifikke beredskabsplaner og straks indberette enhver afbrydelse af disse tjenester, som automatisk klassificeres som væsentlige hændelser.

Det kongelige dekret fastlægger foranstaltninger og mekanismer til koordinering med reglerne om cybersikkerhed og modstandsdygtighed for kritiske enheder (NIS2-direktivet og CER-direktivet), oprettelsen af et koordineringsudvalg for sikkerhed og modstandsdygtighed samt den fremtidige udrulning af digitale platforme til håndtering af hændelser og kommunikation. Samlet set udgør det en væsentlig styrkelse af de forpligtelser vedrørende sikkerhed, kontinuitet og tilsyn, der gælder for telekommunikationssektoren og kritisk digital infrastruktur.

9. Digitaliseringen af økonomien og offentlige tjenester har i væsentlig grad øget afhængigheden af elektroniske



EUROPEAN COMMISSION

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

kommunikationsnet og de digitale infrastrukturer, der understøtter dem. Dette har sat fokus på, at der findes sårbarheder og risici, som ikke udelukkende er begrænset til cybersikkerhedsområdet, men som også påvirker den fysiske sikkerhed og infrastrukturernes evne til at modstå og komme sig efter uheldige hændelser. I denne sammenhæng anser det for nødvendigt at styrke kapaciteten til forebyggelse, håndtering og genopretning i tilfælde af hændelser, der kan bringe tilgængeligheden, integriteten eller driften af elektroniske kommunikationsnet og -tjenester i fare.

I begrundelsen til det kongelige dekret fremhæves en række nylige begivenheder, der har vist, at det er nødvendigt at øge disse infrastrukturers modstandsdygtighed. Blandt disse er naturkatastrofer som vulkanudbruddet i La Palma i 2021 og det kolde lavtrykssystem, der ramte forskellige dele af Spanien i 2024, samt hændelser af ikke-naturlig oprindelse, f.eks. den seneste landsdækkende strømafbrydelse. Disse hændelser viste, at både ekstreme naturfænomener og tekniske fejl eller strømsvigt kan forårsage betydelige forstyrrelser i kommunikationsnetværkene og bringe kontinuiteten i vigtige tjenester for borgerne og offentlige myndigheder i fare.

Desuden medfører digitaliseringen gennemgribende ændringer i telekommunikationsnetværkenes arkitektur og funktionsmåde. Indarbejdelsen af teknologier såsom tingenes internet (IoT), kunstig intelligens (AI), big data, cloudcomputing og virtualisering af tjenester har gjort det muligt at forbedre effektiviteten, konnektiviteten og den økonomiske udvikling, men har samtidig øget systemernes kompleksitet og skabt nye operationelle og sikkerhedsmæssige risici. Derfor er det afgørende, at lovgivningsrammerne udvikles, så disse risici kan forudses, og der sikres et passende niveau af beskyttelse og modstandsdygtighed.

Ud fra et juridisk synspunkt er initiativet hovedsagelig baseret på artikel 63 i lov nr. 11/2022, den generelle telekommunikationslov, om integritet og sikkerhed i elektroniske kommunikationsnet og -tjenester. Den bygger desuden på eksisterende lovgivning om 5G-netsikkerhed, navnlig kongeligt lovdekret 7/2022, kongeligt lovdekret 12/2018 om net- og informationssystemers sikkerhed og kongeligt dekret 443/2024 om godkendelse af den nationale sikkerhedsramme for 5G-net og -tjenester. Uanset ovenstående har disse dekreter ganske vist ført til betydelige fremskridt, men det er nødvendigt at udarbejde en specifik ramme, der på en helhedsorienteret måde tager højde for sikkerheden og modstandsdygtigheden i alle elektroniske kommunikationsnet og -tjenester samt visse digitale infrastrukturer. Endelig forklares det i teksten, at det nye kongelige dekret har til formål at supplere den fremtidige lovgivning i Spanien om kritiske enheders cybersikkerhed og modstandsdygtighed. Som følge heraf vil de forpligtelser, der følger af dekreterne om gennemførelse af NIS2 og CER, fortsat finde fuld anvendelse på cybersikkerhedshændelser og de hændelser, der påvirker digitale net, tjenester og infrastrukturer, og som ikke udtrykkeligt er reguleret i dette kongelige dekret. Således er formålet at sikre sammenhæng mellem de forskellige reguleringsinstrumenter, undgå lovgivningsmæssige overlapninger og etablere et omfattende beskyttelsessystem, der styrker sikkerheden, kontinuiteten og modstandsdygtigheden i telekommunikationsinfrastrukturen og den digitale infrastruktur, som er afgørende for, at det spanske samfund og den spanske økonomi fungerer.

9a. Foranstaltningen er egnet til at nå målet om sikkerhed, modstandsdygtighed og kontinuitet i elektroniske kommunikationsnet og -tjenester samt visse digitale infrastrukturer.

Erfaringer de seneste år har vist, at telekommunikationsnet er afgørende infrastruktur for samfundets funktion, hvilket blev tydeligt under covid-19-pandemien samt i nødsituationer som følge af ekstreme naturbegivenheder, strømafbrydelser eller sikkerhedshændelser, der har påvirket tjenesternes tilgængelighed. I denne situation er det hensigtsmæssigt at indføre en specifik lovramme for at styrke evnen til at forebygge, reagere på og genoprette driften efter hændelser, der kan bringe kontinuiteten i den elektroniske kommunikation i fare.

Dekretet gennemfører bestemmelserne i artikel 63 i lov nr. 11/2022, den generelle lov om telekommunikation. Det supplerer og tilpasser også de lovgivningsmæssige rammer til den teknologiske udvikling og de nye risici, der er forbundet med digitalisering, virtualisering af netværk, cloudcomputing, kunstig intelligens og tingenes internet, hvis udbredelse øger eksponeringen for sårbarheder af både fysisk og digital karakter. I den forbindelse er det kongelige dekret et passende instrument til at præcisere sektorspecifikke forpligtelser, der gør det muligt at anlægge en samlet tilgang til de særlige tekniske og operationelle forhold i telekommunikation.

Foranstaltningens relevans afspejles navnlig i nye forebyggelses- og planlægningsmekanismer, der har til formål at forbedre operatørernes beredskab i krisesituationer. Forpligtelsen til at udarbejde "generelle planer" og "specifikke planer" for hvert netværk eller hver tjeneste samt udarbejdelsen af en "national plan for sikkerhed og modstandsdygtighed" og en "national civil beredskabsplan" gør det muligt at fastlægge specifikke procedurer for risikoidentifikation, forebyggelse, indsats og genopretning.

Tilsvarende er en ajourføring af procedurerne for indberetning af hændelser en relevant foranstaltning til at forbedre de



EUROPEAN COMMISSION

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

kompetente myndigheders kapacitet, når det gælder overvågning og krisestyring. Erfaringen har vist, at der er behov for at tilpasse kriterier, frister og indhold af indberetninger til en mere kompleks teknologisk og operationel virkelighed. Desuden er foranstaltningen velegnet til at styrke beskyttelsen af særligt følsomme tjenester, såsom nødkommunikation via 112-nummeret og offentlige varslingssystemer, ved at pålægge både operatører og alarmcentraler specifikke forpligtelser med hensyn til kontinuitet, redundans og underretning. Dette bidrager til, at nævnte kritiske tjenester opretholdes, selv i situationer, hvor kommunikationsinfrastrukturen forstyrres i alvorlig grad.

Etableringen af samarbejdsmekanismer mellem offentlige myndigheder og nationale og europæiske myndigheder samt oprettelsen af et permanent koordineringsudvalg, der inddrager de forskellige interessenter, er et passende middel til at fremme udveksling af oplysninger, institutionel koordinering og indførelse af bedste praksis inden for sikkerhed og modstandsdygtighed.

Endelig er foranstaltningen i overensstemmelse med den europæiske lovgivningsramme, der følger af NIS2- og CER-direktiverne, hvilket sikrer en passende koordinering med fremtidig national gennemførelseslovgivning og forhindrer lovgivningsmæssige huller i en sektor, der er af strategisk betydning for økonomien og den nationale sikkerhed.

9b. Vedtagelsen af det kongelige dekret imødekommer et reelt og dokumenteret behov for at styrke forebyggelses-, beskyttelses- og genopretningskapaciteten i infrastrukturer, der er blevet afgørende for, at samfundet, økonomien og de offentlige tjenester fungerer.

Digitaliseringen af økonomiske og samfundsmæssige aktiviteter, kombineret med en voksende afhængighed af elektroniske kommunikationsnet og -tjenester, samt begivenheder som vulkanudbruddet på La Palma, det kolde lavtrykssystem, der ramte forskellige dele af landet, eller den nylige strømafbrydelse, har vist, at elektroniske kommunikationsnet og -tjenester er udsat for en lang række risici, der kan udgøre en alvorlig trussel mod væsentlige tjenester for borgere, virksomheder og offentlige myndigheder. Disse hændelser har understreget behovet for at styrke den digitale infrastrukturens modstandsdygtighed og forbedre evnen til at reagere på nødsituationer og kriser.

Denne foranstaltning er nødvendig for at gennemføre og iværksætte artikel 63 i lov nr. 11/2022, den generelle telekommunikationslov, som fastsætter, at operatørerne er forpligtet til at håndtere sikkerhedsrisici på passende vis og sikre integriteten af deres netværk og tjenester. Det er afgørende at udarbejde regler, der mere detaljeret fastlægger de forpligtelser vedrørende planlægning, forebyggelse, indberetning af hændelser, institutionel koordinering og tilsyn, som operatører og andre relevante parter skal opfylde.

Ligeledes begrundes dekretet med, at de gældende rammebestemmelser for indberetning af hændelser delvist er forældede. De nuværende procedurer er ikke længere tilstrækkelige til at håndtere kompleksiteten i de hændelser, der i dag kan påvirke digitale netværk, tjenester og infrastrukturer. Det er nødvendigt at ajourføre typerne af hændelser, kommunikationsprocedurerne og fristerne for indberetning, så de kompetente myndigheder råder over tilstrækkelige og ajourførte oplysninger til at koordinere en hurtig og effektiv indsats i krisesituationer.

Det er desuden nødvendigt at indføre specifikke mekanismer, der skal sikre kontinuiteten i særligt kritiske tjenester, såsom nødopkald via nummeret 112 og offentlige varslingssystemer. Erfaringen viser, at enhver afbrydelse af disse tjenester kan have direkte konsekvenser for beskyttelsen af liv, menneskers fysiske integritet og håndteringen af nødsituationer. Dekretet pålægger derfor både operatører og nødopkaldscentre specifikke forpligtelser med hensyn til planlægning, redundans og operationel kontinuitet.

Desuden er foranstaltningen nødvendig for at forbedre de nationale og europæiske samarbejdsmekanismer og for at oprette et særligt koordineringsudvalg, der skal lette udvekslingen af oplysninger, delingen af erfaringer og fastlæggelsen af fælles procedurer for håndtering af hændelser, som i sagens natur ofte berører flere operatører og infrastrukturer samtidigt.

Endelig er det nødvendigt at sikre, at det spanske retssystem er i overensstemmelse med de nye europæiske rammebestemmelser, der følger af NIS2- og CER-direktiverne. Disse europæiske bestemmelser styrker forpligtelserne vedrørende sikkerhed, risikostyring og modstandsdygtighed i forbindelse med kritisk infrastruktur og pålægger medlemsstaterne at udvikle effektive mekanismer til forebyggelse, påvisning, håndtering og genopretning efter hændelser.

9c. Den foreslåede foranstaltning udgør ikke en urimelig eller uforholdsmæssig byrde i forhold til de tilsigtede mål, da de forpligtelser, den indfører, imødekommer behovet for at sikre sikkerheden, modstandsdygtigheden og kontinuiteten i de infrastrukturer, der er afgørende for, at samfundet, økonomien og de offentlige tjenester fungerer.

Foranstaltningens proportionalitet fremgår først og fremmest af, at mange af de fastsatte forpligtelser allerede indgår i



EUROPEAN COMMISSION

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

telekommunikationsoperatørernes og de digitale infrastrukturforvalteres almindelige praksis inden for risikostyring og forretningskontinuitet. Risikoanalyser, beredskabsplaner, genopretningsprocedurer og tilsynsmekanismer er standardelementer i håndteringen af kritisk infrastruktur og væsentlige tjenester. Det kongelige dekret pålægger ikke oprettelsen af helt nye strukturer, men har til formål at systematisere og ensrette visse forpligtelser for at sikre fælles minimumsstandarder for alle de forpligtede enheder.

Desuden står de påtænkte foranstaltninger i rimeligt forhold til omfanget af de risici, de har til formål at mindske. I lyset af disse risici er kravet om, at der skal foreligge sikkerheds- og beredskabsplaner, backup-mekanismer og procedurer for tidlig indberetning, derfor en rimelig og nødvendig foranstaltning for at minimere skaderne og fremskynde genoprettelsen af tjenesterne.

Dekretet indeholder desuden mekanismer, der gør det muligt at tilpasse forpligtelserne til den enkelte regulerede enheds forhold. De konkrete planer bør udarbejdes under hensyntagen til de særlige forhold, der kendetegner hvert enkelt net, hver enkelt tjeneste eller hver enkelt infrastruktur, således at operatørerne kan fastlægge de mest hensigtsmæssige tekniske og organisatoriske foranstaltninger i overensstemmelse med deres specifikke risici. Denne fleksibilitet undgår, at der pålægges ensartede eller ufleksible løsninger, som kunne medføre unødvendige omkostninger, og fremmer en tilgang, der bygger på effektiv risikostyring.

Hvad angår indberetning af hændelser, begrundes disse forpligtelser i behovet for at råde over ajourførte og pålidelige oplysninger med henblik på at koordinere indsatsen ved hændelser, der kan berøre et stort antal brugere, operatører eller områder. Desuden drejer de krævede oplysninger sig om oplysninger, som operatørerne allerede er forpligtet til at indsamle og administrere internt med henblik på at løse hændelser og sikre kontinuiteten i deres tjenester. De medfører derfor ikke en uforholdsmæssig stor administrativ byrde i forhold til de fordele, de giver med hensyn til koordinering og reaktionsdygtighed.

I rapporten om konsekvensanalysen konkluderes det desuden, at de økonomiske konsekvenser af dekretet er håndterbare og står i rimeligt forhold til den offentlige interesse, den beskytter. Selv om de anslåede finansielle omkostninger for regulerede enheder er på mellem 45 mio. EUR og 90 mio. EUR, er disse omkostninger primært knyttet til investeringer, der har til formål at styrke infrastrukturens modstandsdygtighed og sikre kontinuiteten i væsentlige tjenester. Desuden anslås de nye administrative byrder til ca. 19 276 EUR, hvilket er et lavt tal i forhold til de pågældende virksomheders aktiviteter og økonomi. Desuden har dekretet ingen økonomiske omkostninger for de offentlige myndigheder og har heller ingen væsentlig indvirkning på konkurrencen.

Derfor pålægger foranstaltningen ikke de parter, der er omfattet af den, uforholdsmæssigt store byrder, men fastsætter forpligtelser, der er forholdsmæssige, rimelige og nødvendige for at sikre et højt niveau af sikkerhed og modstandsdygtighed i de elektroniske kommunikationsnet og -tjenester.

10. Henvisninger til grundtekster:

11. Nej

12.

13. Ja

Spaniens strategiske interesser

Elektroniske kommunikationsnet og -tjenester er af afgørende betydning for den nationale sikkerhed, offentlige tjenester, beredskabstjenester, økonomisk aktivitet og territorial samhørighed.

14. Nej

15. Ja

16.

TBT-aspekt: Nej

SPS-aspekt: Nej



EUROPEAN COMMISSION

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

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