REKOMMENDATIONER

KOMMISSIONENS REKOMMENDATION (EU) 2019/534

av den 26 mars 2019

It-säkerhet i 5G-nät

EUROPEISKA KOMMISSIONEN HAR ANTAGIT DENNA REKOMMENDATION

med beaktande av fördraget om Europeiska unionens funktionssätt, särskilt artikel 292, och

av följande skäl:

(1) Kommissionen har erkänt att utbyggnaden av den femte generationens (5G) nätteknik är viktig möjliggörande teknik för framtidens digitala tjänster och högt prioriterat i strategin för den digitala inre marknaden. Kommissionen har antagit en handlingsplan för 5G för att se till att unionen har den nätinfrastruktur som behövs för den digitala omställningen från och med 2020 ([1]).

(2) 5G-näten kommer att bygga på dagens fjärde generation (4G) av nätteknik genom att tillhandahålla kapacitet för nya tjänster och bli den centrala infrastrukturen och möjliggörande tekniken för stora delar av unionens ekonomi. När 5G-näten tagits i drift kommer de att utgöra grunden för en rad tjänster som är nödvändiga för den inre marknadens funktion och för upprätthållandet och driften av vitala samhälleliga och ekonomiska system, exempelvis energi, transporter, banktjänster, hälso- och sjukvård samt industriell processtyrning. Anordnande av demokratiska processer, såsom val, kommer också i allt högre grad att bygga på digital infrastruktur och 5G-nät.

(3) Att många kritiska tjänster kommer att vara beroende av 5G-näten gör följderna av systemomfattande och utbredda störningar särskilt allvarliga. Därför är 5G-nätens it-säkerhet en fråga av strategisk vikt för unionen, i ett skede när it-angreppen ökar och är mer sofistikerade än någonsin.

(4) Den sammankopplade och gränsöverskridande karaktären hos den infrastruktur som ligger till grund för det digitala ekosystemet, liksom de aktuella hotens gränsöverskridande karaktär, innebär att alla betydande sårbarheter och it-säkerhetsincidenter som påverkar 5G-nät i en medlemsstat får följder för unionen som helhet. Därför bör åtgärder vidtas för att underbygga en hög gemensam it-säkerhetsnivå i 5G-näten.

(5) Behovet av åtgärder på unionsnivå har bekräftats av medlemsstaterna. Europeiska rådet såg i sina slutsatser från mötet den 21 mars 2019 fram emot kommissionens rekommendation om en samordnad strategi i fråga om 5G-nätens säkerhet ([2]).

(6) Att säkerställa unionens oberoende bör vara ett viktigt mål, i fullständig överensstämmelse med de europeiska värdena om öppenhet och tolerans ([3]). Utländska investeringar i strategiska sektorer, förvärv av kritisk materiel, teknik och infrastruktur i unionen samt leveranser av kritisk utrustning kan också utgöra hot mot unionens säkerhet.

(7) It-säkerheten i 5G-näten har avgörande betydelse för unionens strategiska oberoende, vilket framhålls i det gemensamma meddelandet *EU och Kina – En strategisk hållning* ([4]).

(8) Europaparlamentet uppmanar även i sin resolution om säkerhetshot kopplade till Kinas ökande teknologiska närvaro i EU kommissionen och medlemsstaterna att vidta åtgärder på unionsnivå ([5]).

(9) Den här rekommendationen inriktas på it-säkerhetsrisker i 5G-nät genom att fastställa vägledning om lämpliga riskbedömnings- och riskhanteringsåtgärder på nationell nivå, om utveckling av en samordnad europeisk riskbedömning och om inrättande av en process för utveckling av en gemensam verktygslåda med de bästa riskhanteringsåtgärderna.

(10) Det finns stark unionslagstiftning om skydd av elektroniska kommunikationsnät.

([1]) COM(2016) 588 final.
([2]) Europeiska rådets slutsatser av den 21 och 22 mars 2019.
([3]) Tillståndet i unionen 2018 – Tid för ett suveränt EU, 12 september 2018.
([4]) JOIN(2019) 5 final.
([5]) http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2019-0156+0+DOC+PDF+V0//SV

(11) Unionens bestämmelser om elektronisk kommunikation ([6]) främjar konkurrens, inre marknad och slutanvändarnas intressen, och genom den europeiska kodexen för elektronisk kommunikation ([7]) eftersträvas ett kompletterande konnektivitetsmål som anges i resultattermer: utbredd tillgång till och användning av fasta och mobila högkapacitetsuppkopplingar för alla enskilda och företag i unionen, samtidigt som de medborgerliga intressena skyddas. Enligt direktiv 2002/21/EG ska medlemsstaterna säkerställa att de allmänna kommunikationsnätens integritet och säkerhet upprätthålls, förenat med skyldigheten att säkerställa att företag som tillhandahåller allmänna kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster vidtar lämpliga tekniska och organisatoriska åtgärder för att på ett tillfredsställande sätt skydda säkerheten för sina nät eller tjänster. Vidare föreskrivs att de behöriga nationella regleringsmyndigheterna ska ha befogenheter, inbegripet befogenheter att utfärda bindande instruktioner, för att se till att sådana skyldigheter efterlevs.

(12) Dessutom kan medlemsstaterna enligt Europaparlamentets och rådets direktiv 2002/20/EG ([8]) förena den generella auktorisationen med villkor för allmänna näts säkerhet mot olovlig åtkomst i syfte att skydda telehemligheten i enlighet med Europaparlamentets och rådets direktiv 2002/58/EG ([9]).

(13) Till stöd för genomförandet av dessa skyldigheter har unionen inrättat ett antal samarbetsorgan. Europeiska unionens byrå för nät- och informationssäkerhet (Enisa), kommissionen, medlemsstaterna och de nationella regleringsmyndigheterna har tagit fram tekniska riktlinjer för de nationella regleringsmyndigheternas rapportering av incidenter, säkerhetsåtgärder, hot och resurser ([10]). Den samarbetsgrupp som inrättats genom Europaparlamentets och rådets direktiv (EU) 2016/1148 ([11]) (nedan kallad *samarbetsgruppen*) sammanför de behöriga myndigheterna för att understödja och underlätta samarbetet, särskilt genom att tillhandahålla strategisk vägledning för verksamheten i nätverket av it-incidentcentrum, som underlättar det operativa samarbetet på teknisk nivå.

(14) De kommande EU-reglerna om it-säkerhetscertifiering ([12]) bör på ett väsentligt sätt bidra till en jämn nivå på säkerheten. De bör göra det möjligt att utveckla system för it-säkerhetscertifiering för att tillgodose behoven hos användare av 5G-relaterad utrustning och programvara. Den här infrastrukturens kritiska betydelse bör leda till att högsta prioritet ges åt utvecklingen av europeiska system för it-säkerhetscertifiering av informations- och kommunikationstekniska produkter, tjänster och processer som används i 5G-nät. Medlemsstaterna och marknadsaktörerna bör aktivt engagera sig i utvecklingen av sådana certifieringssystem, även genom att stödja fastställandet av särskilda skyddsprofiler för 5G-nät.

(15) I avsaknad av harmoniserad unionslagstiftning får medlemsstaterna i nationella tekniska föreskrifter, antagna i överensstämmelse med unionsrätten, föreskriva att ett europeiskt system för it-säkerhetscertifiering ska vara obligatoriskt. Medlemsstaterna kan också använda europeiska system för it-säkerhetscertifiering vid offentlig upphandling och vid tillämpningen av Europaparlamentets och rådets direktiv 2014/24/EU ([13]), och kan stödja utvecklingen av olika former av assistans, t.ex. en knutpunkt för assistans, för offentliga enheters upphandling av it-säkerhetslösningar.

(16) Ett starkt dataskydd och skydd av den personliga integriteten är ett viktigt inslag i säkerheten för 5G-nät. Det finns även regler på unionsnivå om säker behandling av personuppgifter, även inom elektronisk kommunikation. I den allmänna dataskyddsförordningen ([14]) fastställs skyldigheten att personuppgifter ska behandlas så att deras säkerhet garanteras, inbegripet förhindrande av otillåten åtkomst till eller användning av personuppgifter och den utrustning som används för behandlingen. I direktivet om integritet och elektronisk kommunikation anges

([6]) Europaparlamentets och rådets direktiv 2002/21/EG av den 7 mars 2002 om ett gemensamt regelverk för elektroniska kommunikationsnät och kommunikationstjänster (ramdirektiv) (EGT L 108, 24.4.2002, s. 33), med särdirektiv.

([7]) Europaparlamentets och rådets direktiv (EU) 2018/1972 av den 11 december 2018 om inrättande av en europeisk kodex för elektronisk kommunikation (EUT L 321, 17.12.2018, s. 36).

([8]) Europaparlamentets och rådets direktiv 2002/20/EG av den 7 mars 2002 om auktorisation för elektroniska kommunikationsnät och kommunikationstjänster (auktorisationsdirektiv) (EGT L 108, 24.4.2002, s. 21).

([9]) Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation) (EGT L 201, 31.7.2002, s. 37).

([10]) https://resilience.enisa.europa.eu/article-13

([11]) Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen (EUT L 194, 19.7.2016, s. 1).

([12]) Förslag till Europaparlamentets och rådets förordning om Enisa, ”EU:s cybersäkerhetsbyrå”, och om upphävande av förordning (EU) nr 526/2013, och om cybersäkerhetscertifiering av informations- och kommunikationsteknik (”cybersäkerhetsakten”) (COM(2017) 477 final – 2017/0225 (COD)).

([13]) Europaparlamentets och rådets direktiv 2014/24/EU av den 26 februari 2014 om offentlig upphandling och om upphävande av direktiv 2004/18/EG (EUT L 94, 28.3.2014, s. 65).

([14]) Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) (EUT L 119, 4.5.2016, s. 1).

särskilda regler om skydd av telehemligheten och skydd av slutanvändarnas terminalutrustning. Enligt det direktivet är tjänsteleverantörerna också skyldiga att vidta lämpliga tekniska och organisatoriska åtgärder för att se till att deras tjänster är säkra.

(17) Unionen har också antagit en rättsakt som ska skydda kritisk infrastruktur och teknik, bl.a. inom kommunikationssektorn, genom att ge medlemsstaterna möjlighet att granska utländska direktinvesteringar med avseende på säkerhet eller allmän ordning, och genom att det inrättas en samarbetsstruktur där medlemsstaterna och kommissionen kan utbyta information och ta upp farhågor rörande enskilda investeringar ([15]).

(18) Medlemsstaterna och operatörerna håller för närvarande på att vidta omfattande förberedelser för att möjliggöra den storskaliga driftsättningen av 5G-näten. Ett antal medlemsstater har uttryckt oro för eventuella säkerhetsrisker i 5G-nät i samband med förfaranden för beviljande av rätt att använda de radiospektrumband som 5G-näten tilldelats ([16]), och har övervägt åtgärder mot dessa risker.

(19) Vid hanteringen av it-säkerhetsrisker i 5G-nät bör både tekniska och andra faktorer beaktas: Tekniska faktorer kan omfatta sårbarheter i fråga om it-säkerhet som kan utnyttjas för att få obehörig åtkomst till information (it-spionage, oavsett om det är av ekonomiska eller politiska skäl) eller för andra fientliga syften (it-angrepp avsedda att störa eller förstöra system och data). Viktiga aspekter som bör beaktas är behovet av att skydda näten under hela deras livscykel och behovet av att all relevant utrustning omfattas, inbegripet under 5Gnätens konstruktion, utveckling, upphandling, utbyggnad, drift och underhåll.

(20) Andra faktorer kan inbegripa lagfästa krav och andra krav på leverantörer av utrustning för informations- och kommunikationsteknik. Vid en bedömning av sådana faktorers betydelse bör hänsyn tas till bland annat den totala risken för påverkan från ett tredjeland, särskilt med avseende på dess statsskick, avsaknad av samarbetsavtal om säkerhet eller liknande arrangemang i fråga om dataskydd mellan unionen och det aktuella tredjelandet, exempelvis beslut om adekvat skyddsnivå, eller huruvida landet är part i multilaterala, internationella eller bilaterala avtal om it-säkerhet, bekämpning av it-brottslighet eller dataskydd.

(21) Som ett viktigt steg i utvecklingen av en unionsmodell för it-säkerhet i 5G-nät bör en riskbedömning genomföras på nationell nivå. Detta hjälper medlemsstaterna att anpassa sina nationella åtgärder i fråga om säkerhetskrav och riskhantering enligt bedömningen.

(22) Samordning bör utvecklas för att de åtgärder som syftar till att hantera sådana it-hot ska bli verkningsfulla, eftersom de åtgärderna är nödvändiga för att den inre marknaden ska fungera smidigt och för att skydda personuppgifter och personlig integritet.

(23) De nationella riskbedömningarna bör tjäna som utgångspunkt för en samordnad unionsriskbedömning, bestående av en hotbildskartläggning och en gemensam översyn som utförs av medlemsstaterna med stöd av kommissionen och i samarbete med Europeiska unionens byrå för nät- och informationssäkerhet (Enisa).

(24) Med beaktande av medlemsstaternas och unionens riskbedömningar bör samarbetsgruppen sammanställa en verktygslåda för olika slags it-säkerhetsrisker och möjliga åtgärder för motverkande av riskerna på områden som certifiering, provning och åtkomstkontroll. Samarbetsgruppen bör också ange tänkbara särskilda åtgärder för att hantera risker som en eller flera medlemsstater utpekar. Samarbetsgruppen bör få stöd av Europeiska unionens byrå för nät- och informationssäkerhet (Enisa), Europol, Organet för europeiska regleringsmyndigheter för elektronisk kommunikation (Berec) samt EU:s underrättelse- och lägescentral. Denna verktygslåda bör fungera som underlag till kommissionen när det gäller att utveckla gemensamma minimikrav för att säkerställa en hög nivå av it-säkerhet i 5G-nät i hela unionen.

(25) När åtgärder vidtas mot it-säkerhetsrisker bör hänsyn tas till främjande av it-säkerhet genom diversifiering av leverantörer när enskilda nät byggs upp.

([15]) Europaparlamentets och rådets förordning (EU) 2019/452 av den 19 mars 2019 om upprättande av en ram för granskning av utländska direktinvesteringar i unionen (EUT L 79I, 21.3.2019, s. 1).

([16]) Utauktionering av minst ett spektrumband planeras äga rum 2019 i elva medlemsstater: Belgien, Tjeckien, Tyskland, Grekland, Frankrike, Irland, Ungern, Litauen, Nederländerna, Österrike och Portugal. Ytterligare sex auktioner planeras äga rum 2020: Spanien, Litauen (andra frekvenser), Malta, Slovakien, Polen och Förenade kungariket. *Källa:* http://5gobservatory.eu/observatory-overview/observatory-reports/.

(26) Denna rekommendation bör inte påverka tillämpningen av medlemsstaternas behörighet i fråga om verksamhet som rör allmän säkerhet, försvar, nationell säkerhet eller statens verksamhet på straffrättens område, inbegripet medlemsstaternas rätt att utestänga leverantörer från sina marknader av skäl som rör nationell säkerhet.

HÄRIGENOM REKOMMENDERAS FÖLJANDE.

I. **MÅL**

1. För att stödja framväxten av en unionsmodell för säkerställande av it-säkerhet i 5G-nät anges i denna rekommendation de åtgärder som bör vidtas så att

   a) medlemsstaterna kan bedöma de it-säkerhetsrisker som påverkar 5G-nät på nationell nivå och vidta nödvändiga säkerhetsåtgärder,

   b) medlemsstaterna och relevanta unionsinstitutioner, unionsbyråer och unionsorgan gemensamt kan utveckla en samordnad unionsriskbedömning som bygger på de nationella riskbedömningarna,

   c) den samarbetsgrupp som inrättats enligt direktiv (EU) 2016/1148 (nedan kallad *samarbetsgruppen*) kan ange en gemensam uppsättning tänkbara åtgärder för att minska it-säkerhetsrisker förknippade med den infrastruktur som ligger till grund för det digitala ekosystemet, särskilt 5G-näten.

II. **DEFINITIONER**

2. I denna rekommendation gäller följande definitioner:

   a) *5G-nät*: en uppsättning av alla relevanta nätinfrastrukturelement för mobil och trådlös kommunikationsteknik som används för konnektivitet och mervärdestjänster med avancerade prestanda, i form av t.ex. mycket höga datahastigheter och mycket hög datakapacitet, kommunikation med låg latens, ultrahög tillförlitlighet eller stöd till ett stort antal anslutna enheter. Detta kan inbegripa äldre nätelement som bygger på tidigare generationer av mobil och trådlös kommunikationsteknik såsom 4G eller 3G. 5G-näten bör anses inbegripa alla relevanta delar av nätet.

   b) *infrastruktur som ligger till grund för det digitala ekosystemet*: infrastruktur som används för att möjliggöra digitalisering i ett brett spektrum av kritiska tillämpningar i ekonomin och samhället.

III. **INSATSER PÅ NATIONELL NIVÅ**

3. Senast den 30 juni 2019 bör medlemsstaterna ha genomfört en riskbedömning av 5G-nätinfrastrukturen, vilket inbegriper att kartlägga de känsligaste elementen där säkerhetsbrister skulle få betydande negativa konsekvenser. Senast samma datum bör medlemsstaterna även ha sett över de säkerhetskrav och riskhanteringsmetoder som gäller på nationell nivå, för att ta hänsyn till it-säkerhetshot som kan uppstå på grund av i) tekniska faktorer, såsom 5G-nätens särskilda tekniska egenskaper, och ii) andra faktorer, såsom den rättsliga och politiska ram som leverantörer av informations- och kommunikationsteknik kan vara föremål för i tredjeländer.

4. På grundval av denna nationella riskbedömning och översyn och med beaktande av pågående samordnade åtgärder på unionsnivå bör medlemsstaterna göra följande:

   a) Uppdatera de säkerhetskrav och riskhanteringsmetoder som är tillämpliga på 5G-nät.

   b) Uppdatera de relevanta skyldigheter som gäller för företag som tillhandahåller allmänna kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster enligt artiklarna 13a och 13b i direktiv 2002/21/EG.

   c) Förena generella auktorisationer med villkor rörande allmänna näts säkerhet mot olovlig åtkomst och be om åtaganden från företag som deltar i kommande förfaranden för tilldelning av rätt att använda radiofrekvenser i 5G-banden vad gäller efterlevnad av säkerhetskrav för nät enligt direktiv 2002/20/EG.

   d) Vidta andra förebyggande åtgärder för att motverka potentiella it-säkerhetsrisker.

5. Åtgärder enligt punkt 4 bör omfatta utökade skyldigheter för leverantörer och operatörer att trygga känsliga nätdelars säkerhet och skyldighet att i förekommande fall exempelvis lämna relevant information till behöriga nationella myndigheter om planerade ändringar av elektroniska kommunikationsnät och krav att vissa informationstekniska komponenter och system ska provas i förväg av nationella kontroll- och certifieringslaboratorier med avseende på säkerhet och integritet.

6. Gemensamma säkerhetsgranskningar bör genomföras av två eller flera medlemsstater, som använder och delar på lämplig teknisk expertis och resurser som avser den infrastruktur som ligger till grund för det digitala ekosystemet och 5G-näten, till exempel när samma företag driver eller bygger nätinfrastruktur i flera medlemsstater eller om det finns stora likheter mellan nätkonfigurationerna. Europeiska byrån för nät- och informationssäkerhet (Enisa), Europol och Organet för europeiska regleringsmyndigheter för elektronisk kommunikation (Berec) bör ge förtur till ansökningar om stöd från medlemsstaterna på detta område. Resultaten av dessa granskningar bör överlämnas till samarbetsgruppen och nätverket av enheter för hantering av it-säkerhetsincidenter.

IV. SAMORDNADE ÅTGÄRDER PÅ UNIONSNIVÅ

7. För att ta fram en samordnad strategi för it-säkerhetsrisker i 5G-nät bör medlemsstaterna senast den 30 april 2019 inleda en särskild verksamhetsdel inom samarbetsgruppen. Medlemsstaterna bör uppmana de relevanta myndigheterna att vid behov delta i samarbetsgruppens arbete.

Samordnad europeisk riskbedömning

8. Medlemsstaterna bör utbyta information med varandra och med relevanta unionsorgan i syfte att bygga upp en gemensam uppfattning om befintliga och potentiella it-säkerhetsrisker i 5G-nät.

9. Medlemsstaterna bör översända sina nationella riskbedömningar till kommissionen och till Europeiska unionens byrå för nät- och informationssäkerhet (Enisa) senast den 15 juli 2019.

10. Europeiska unionens byrå för nät- och informationssäkerhet (Enisa) bör genomföra en särskild hotbildskartläggning för 5G-nät. Samarbetsgruppen och nätverket av enheter för hantering av it-säkerhetsincidenter, som inrättats i enlighet med direktiv (EU) 2016/1148, bör stödja denna process.

11. Med beaktande av allt detta bör medlemsstaterna med stöd av kommissionen och i samarbete med Europeiska unionens byrå för nät- och informationssäkerhet (Enisa) senast den 1 oktober 2019 ha genomfört en gemensam unionsomfattande översyn av riskerna med den infrastruktur som ligger till grund för det digitala ekosystemet, särskilt 5G-näten.

12. Denna gemensamma översyn bör särskilt inriktas på att analysera risker med särskilt känsliga eller sårbara element i 5G-nätens kärnor, på drifts- och underhållscentraler samt på 5G-accessnätselement som används i industriella tillämpningar.

13. I ett andra skede bör denna gemensamma översyn utökas till andra strategiska länkar i den digitala värdekedjan.

Gemensam unionsverktygslåda för riskhantering

14. Under arbetet i samarbetsgruppen bör bästa praxis på nationell nivå kartläggas enligt punkt 4. På grundval av denna bästa nationella praxis bör en verktygslåda av lämpliga, effektiva och proportionella riskhanteringsåtgärder för att motverka de utpekade it-säkerhetsriskerna på nationell nivå och unionsnivå överenskommas senast den 31 december 2019, för att ge kommissionen vägledning vid utvecklingen av gemensamma minimikrav för en hög it-säkerhetsnivå i 5G-nät i hela unionen.

15. Verktygslådan bör omfatta

a) en genomgång av de typer av risker som kan påverka it-säkerheten i 5G-nät (t.ex. risker i leveranskedjan, risker på grund av sårbarheter i programvaran, risker med åtkomstkontroll samt risker på grund av den rättsliga och politiska ram som leverantörer av informations- och kommunikationsteknik kan vara föremål för i tredjeländer), och

b) en uppsättning riskminskande åtgärder (t.ex. tredjepartscertifiering av maskinvara, programvara och tjänster, formell maskinvaru- och programvaruprovning eller bedömning av överensstämmelse, rutiner för att se till att åtkomstkontroll finns och tillämpas samt identifiering av produkter, tjänster eller leverantörer som eventuellt anses osäkra). Åtgärderna bör inriktas på alla typer av säkerhetsrisker som utpekas i en eller flera medlemsstater efter riskbedömningen.

16. När väl europeiska system för it-säkerhetscertifiering för 5G-nät har utvecklats bör medlemsstaterna i enlighet med unionslagstiftningen anta nationella tekniska föreskrifter om obligatorisk certifiering av informations- och kommunikationstekniska produkter, tjänster eller system som omfattas av dessa certifieringssystem.

17. Medlemsstaterna bör i samarbete med kommissionen fastställa villkor för allmänna näts säkerhet mot olovlig åtkomst som generella auktorisationer kan förenas med, och säkerhetskrav för nät som kan ställas när man ber om åtaganden från företag som deltar i kommande förfaranden för tilldelning av rätt att använda radiofrekvenser i 5G-banden vad gäller efterlevnad av säkerhetskrav för nät enligt direktiv 2002/20/EG. Dessa bör i möjligaste mån återspeglas i sådana åtgärder som vidtas enligt punkt 4 c.

18. Medlemsstaterna bör samarbeta med kommissionen för att ta fram särskilda säkerhetskrav som kan tillämpas i samband med offentlig upphandling som avser 5G-nät. Detta bör omfatta obligatoriska krav på att genomföra system för it-säkerhetscertifiering i offentlig upphandling, i den mån sådana system ännu inte är bindande för alla leverantörer och operatörer.

V. **ÖVERSYN**

19. Medlemsstaterna bör samarbeta med kommissionen för att bedöma effekterna av denna rekommendation senast den 1 oktober 2020, i syfte att fastställa lämpliga vägar framåt. Vid denna bedömning bör resultaten av den samordnade unionsriskbedömningen och unionsverktygslådan beaktas.

Utfärdad i Strasbourg den 26 mars 2019.

På kommissionens vägnar

Julian KING

Ledamot av kommissionen