HENSTILLINGER

KOMMISSIONENS HENSTILLING (EU) 2019/534

af 26. marts 2019

Cybersikkerheden i forbindelse med 5G-net

EUROPA-KOMMISSIONEN HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde, særlig artikel 292, og

ud fra følgende betragtninger:

(1) Kommissionen har anerkendt, at etableringen af femte generation (5G) af netteknologier åbner store muligheder for fremtidige digitale tjenester og prioriteres højt i strategien for et digitalt indre marked. Kommissionen vedtog 5G-handlingsplanen for at sikre, at Unionen har den konnektivitetsinfrastruktur, der er nødvendig for den digitale omstilling fra og med 2020 ([1]).

(2) 5G-nettene vil bygge videre på den nuværende fjerde generation (4G) af netteknologier ved at sikre ny kapacitet og blive den centrale infrastruktur og katalysator for store dele af Unionens økonomi. Når de er indført, vil 5G-nettene udgøre rygraden i en lang række tjenesteydelser, som er afgørende for det indre markeds funktion og for opretholdelsen og driften af vitale samfundsmæssige og økonomiske funktioner — f.eks. energi, transport, bankvæsen og sundhed samt industrielle kontrolsystemer. Tilrettelæggelsen af demokratiske processer, såsom valg, vil også blive mere og mere afhængig af digital infrastruktur og af 5G-net.

(3) Mange kritiske tjenesters afhængighed af 5G-nettene vil medføre særlig alvorlige konsekvenser i tilfælde af systemiske og omfattende forstyrrelser. Som følge heraf er det af strategisk betydning for Unionen at sikre cybersikkerheden i forbindelse med 5G-net på et tidspunkt, hvor cyberangreb er hyppigere og mere sofistikerede end nogensinde før.

(4) Den indbyrdes forbundne og tværnationale karakter af de infrastrukturer, der understøtter det digitale økosystem, og de involverede truslers grænseoverskridende karakter betyder, at alle væsentligt svage punkter og/eller cybersikkerhedshændelser i forbindelse med 5G-nettet i en enkelt medlemsstat vil påvirke hele Unionen. Derfor bør der træffes foranstaltninger for at understøtte et højt fælles cybersikkerhedsniveau for 5G-net.

(5) Behovet for en indsats på EU-plan er blevet bekræftet af medlemsstaterne. Det Europæiske Råd ser i sine konklusioner af 21. marts 2019 frem til en henstilling fra Kommissionen om en fælles tilgang til sikkerheden i forbindelse med 5G-net ([2]).

(6) Det bør være et vigtigt mål at sikre europæisk suverænitet under fuld overholdelse af europæiske værdier som åbenhed og tolerance ([3]). Udenlandske investeringer i strategiske sektorer, erhvervelse af kritiske aktiver, teknologier og infrastrukturer i Unionen samt levering af kritisk udstyr kan også udgøre en sikkerhedsmæssig risiko for Unionen.

(7) Cybersikkerheden i forbindelse med 5G-net er afgørende for at sikre Unionens strategiske autonomi, som det fremgår af den fælles meddelelse »Forbindelserne mellem EU og Kina i et strategisk perspektiv« ([4]).

(8) Europa-Parlamentet opfordrer i sin beslutning om sikkerhedstrusler forbundet med den stigende kinesiske teknologiske tilstedeværelse i EU ligeledes Kommissionen og medlemsstaterne til at træffe foranstaltninger på EU-plan ([5]).

(9) Nærværende henstilling imødegår cybersikkerhedsrisiciene i 5G-net ved at fastsætte retningslinjer for passende foranstaltninger til risikoanalyse og -håndtering på nationalt plan, for udvikling af en koordineret europæisk risikovurdering og for fastlæggelse af en proces til at udvikle en fælles værktøjskasse med de bedste risikohåndteringsforanstaltninger.

(10) Der foreligger en stærk EU-lovramme til beskyttelse af elektroniske kommunikationsnet.

([1]) COM(2016) 588 final.
([2]) Det Europæiske Råds konklusioner af 21. og 22. marts 2019.
([3]) Tale om Unionens tilstand 2018 — Tid til europæisk suverænitet, den 12. september 2018.
([4]) JOIN(2019) 5 final.
([5]) www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2019-0156+0+DOC+PDF+V0//DA.

(11) Unionens ramme for elektronisk kommunikation ([6]) fremmer konkurrencen, det indre marked og slutbrugernes interesser og forfølger via den europæiske kodeks for elektronisk kommunikation ([7]) et yderligere konnektivitetsmål udtrykt i resultater: udbredt adgang til og brug af fast- og mobilnet med meget høj kapacitet for alle Unionens borgere og virksomheder, samtidig med at borgernes interesser beskyttes. I henhold til direktiv 2002/21/EF skal medlemsstaterne sikre, at de offentlige kommunikationsnets integritet og sikkerhed opretholdes, herunder er de forpligtede til at sikre, at virksomheder, der udbyder offentlige kommunikationsnet eller offentligt tilgængelige elektroniske kommunikationstjenester, træffer tekniske og organisatoriske foranstaltninger for på passende vis at styre risiciene for sikkerheden i deres net og tjenester. Det fastsættes også, at de kompetente nationale tilsynsmyndigheder har beføjelser, herunder beføjelse til at udstede bindende instrukser, for at sikre, at disse forpligtelser overholdes.

(12) Desuden giver Europa-Parlamentets og Rådets direktiv 2002/20/EF ([8]) medlemsstaterne mulighed for at knytte vilkår vedrørende sikring af offentlige net mod uautoriseret adgang til den generelle tilladelse med henblik på at beskytte kommunikationshemmeligheden i overensstemmelse med Europa-Parlamentets og Rådets direktiv 2002/58/EF ([9]).

(13) For at støtte gennemførelsen af disse forpligtelser har Unionen oprettet en række samarbejdsorganer. Agenturet for Net- og Informationssikkerhed (ENISA) har sammen med Kommissionen, medlemsstaterne og de nationale tilsynsmyndigheder udarbejdet tekniske retningslinjer for de nationale tilsynsmyndigheder vedrørende indberetning af hændelser, sikkerhedsforanstaltninger, trusler og aktiver ([10]). Den samarbejdsgruppe, der er nedsat ved direktiv (EU) 2016/1148 ([11]) (»samarbejdsgruppen«), samler de kompetente myndigheder for at støtte og fremme samarbejdet, navnlig ved at give strategisk vejledning om aktiviteterne i netværket af enheder, der håndterer IT-sikkerhedshændelser, og som på teknisk plan letter det operationelle samarbejde.

(14) Den fremtidige europæiske ramme for cybersikkerhedscertificering ([12]) bør være et væsentligt hjælperedskab til at sikre et ensartet sikkerhedsniveau Den bør gøre det muligt at udvikle cybersikkerhedscertificeringsordninger for at opfylde behovene hos brugere af 5G-relateret udstyr og software. Disse infrastrukturers afgørende betydning bør gøre det til en umiddelbar prioritet at opstille relevante europæiske cybersikkerhedscertificeringsordninger for informations- og kommunikationsteknologiske produkter, tjenester eller processer, der anvendes til 5G-net. Medlemsstaterne og markedsaktørerne bør deltage aktivt i udviklingen af disse certificeringsordninger, herunder ved at yde støtte til fastlæggelse af specifikke beskyttelsesprofiler for 5G-net.

(15) I mangel af harmonisering på EU-plan kan medlemsstaterne ved hjælp af nationale tekniske forskrifter vedtaget i overensstemmelse med EU-retten fastsætte, at en europæisk cybersikkerhedscertificeringsordning bør være obligatorisk. Medlemsstaterne kan også anvende europæiske cybersikkerhedscertificeringsordninger i forbindelse med offentlige udbud og direktiv 2014/24/EU ([13]) og kan understøtte udviklingen af hjælpemekanismer — som f. eks. en støtteplatform — til offentlige indkøberes køb af cybersikkerhedsløsninger.

(16) En høj beskyttelse af personoplysninger og privatlivets fred udgør en vigtig del af 5G-nettets sikkerhed. Der er også på EU-plan fastlagt regler for at garantere sikker behandling af personoplysninger, herunder i forbindelse med elektronisk kommunikation. I den generelle forordning om databeskyttelse ([14]) fastsættes forpligtelsen til at behandle personoplysninger på en måde, der holder dem sikre, herunder for at forhindre uautoriseret adgang til

([6]) Europa-Parlamentets og Rådets direktiv 2002/21/EF af 7. marts 2002 om fælles rammebestemmelser for elektroniske kommunikationsnet og -tjenester (rammedirektivet) (EFT L 108 af 24.4.2002, s. 33) og særdirektiverne.

([7]) Europa-Parlamentets og Rådets direktiv (EU) 2018/1972 af 11. december 2018 om oprettelse af en europæisk kodeks for elektronisk kommunikation (EUT L 321 af 17.12.2018, s. 36).

([8]) Europa-Parlamentets og Rådets direktiv 2002/20/EF af 7. marts 2002 om tilladelser til elektroniske kommunikationsnet og -tjenester (tilladelsesdirektivet) (EFT L 108 af 24.4.2002, s. 21).

([9]) Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (direktiv om databeskyttelse inden for elektronisk kommunikation)(EFT L 201 af 31.7.2002, s. 37).

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

([11]) Europa-Parlamentets og Rådets direktiv (EU) 2016/1148 af 6. juli 2016 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen (EUT L 194 af 19.7.2016, s. 1).

([12]) Forslag til Europa-Parlamentets og Rådets Forordning om ENISA, »EU's Agentur for Cybersikkerhed«, om ophævelse af forordning (EU) nr. 526/2013 og om cybersikkerhedscertificering af informations- og kommunikationsteknologi (»forordningen om cybersikkerhed«), COM(2017) 477 final — 2017/0225 (COD).

([13]) Europa-Parlamentets og Rådets direktiv 2014/24/EU af 26. februar 2014 om offentlige udbud og om ophævelse af direktiv 2004/18/EF (EUT L 94 af 28.3.2014, s. 65).

([14]) Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse) (EUT L 119 af 4.5.2016, s. 1).

eller brug af personoplysninger og databehandlingsudstyret. Direktivet om databeskyttelse inden for elektronisk kommunikation indeholder nærmere regler om beskyttelse af kommunikationshemmeligheden og slutbrugernes terminaludstyr. Heri pålægges tjenesteudbyderne også forpligtelser til at træffe passende tekniske og organisatoriske foranstaltninger for at beskytte deres tjenester.

(17) Unionen har også vedtaget et instrument, der vil beskytte kritisk infrastruktur og kritiske teknologier såsom dem, der anvendes i kommunikation, ved at give medlemsstaterne mulighed for at screene udenlandske direkte investeringer af hensyn til sikkerheden eller den offentlige orden og ved at skabe en samarbejdsmekanisme, hvor medlemsstaterne og Kommissionen kan udveksle oplysninger og udtrykke betænkeligheder vedrørende bestemte investeringer ([15]).

(18) Medlemsstaterne og operatørerne er i øjeblikket ved at træffe vigtige forberedende foranstaltninger, der skal muliggøre en storstilet udrulning af 5G-net. Flere medlemsstater har udtrykt bekymring over potentielle sikkerhedsrisici vedrørende 5G-net i forbindelse med gennemførelsen af procedurerne for tildelingen af brugsrettigheder til de frekvensbånd, der er udpeget til 5G-net ([16]), og har undersøgt foranstaltninger til håndtering af disse risici.

(19) Ved håndteringen af cybersikkerhedsrisiciene i 5G-net bør der tages hensyn til både tekniske og andre faktorer. Tekniske faktorer kan omfatte cybersikkerhedssårbarheder, som kan udnyttes til at opnå uautoriseret adgang til oplysninger (cyberspionage af enten økonomiske eller politiske grunde) eller andre skadelige formål (cyberangreb med det formål at forårsage afbrydelser eller ødelæggelser af systemer og data). Det er vigtigt at se på behovet for dels at beskytte nettene igennem hele deres livscyklus, dels at dække alt relevant udstyr, herunder i forbindelse med design, udvikling, anskaffelse, udrulning, drift og vedligeholdelse af 5G-nettene.

(20) Andre faktorer kan omfatte lovgivningsmæssige eller andre krav til leverandører af informations- og kommunikationsteknologiudstyr. I en vurdering af sådanne faktorers betydning vil der bl.a. skulle tages højde for den samlede risiko for påvirkning fra et tredjeland, navnlig med hensyn til dets forvaltningsmodel, mangel på sikkerhedssamarbejdsaftaler eller lignende ordninger for databeskyttelse såsom beslutninger om et tilstrækkeligt beskyttelsesniveau mellem Unionen og det pågældende tredjeland, landets deltagelse i multilaterale, internationale eller bilaterale cybersikkerhedsaftaler, bekæmpelse af cyberkriminalitet samt databeskyttelse.

(21) I udviklingen af en EU-tilgang til sikkerheden i forbindelse med 5G-net bør der som et vigtigt skridt foretages og færdiggøres en risikovurdering på nationalt plan. Dette vil hjælpe medlemsstaterne med på baggrund af denne vurdering at tilpasse de nationale foranstaltninger vedrørende sikkerhedskrav og risikohåndterring.

(22) Der bør foretages en koordinering for at sikre effektive foranstaltninger til håndtering af disse cybertrusler, hvilket har afgørende betydning for et velfungerende indre marked og for beskyttelse af personoplysninger og privatlivets fred.

(23) De nationale risikovurderinger bør danne grundlag for en koordineret EU-risikovurdering, der består af en kortlægning af trusselsbilledet og en fælles evaluering, der med støtte fra Kommissionen foretages af medlemsstaterne sammen med Det Europæiske Agentur for Cybersikkerhed (ENISA).

(24) Samarbejdsgruppen bør under hensyntagen til de nationale og EU's risikovurderinger skabe en værktøjskasse til afdækning af forskellige typer cybersikkerhedsrisici og mulige foranstaltninger til at afbøde risiciene på områder som certificering, afprøvning og adgangskontrol. Den bør også indkredse eventuelle særlige tiltag, der egner sig til håndtering af risici, som en eller flere medlemsstater har udpeget. Samarbejdsgruppen bør trække på støtte fra Det Europæiske Agentur for Cybersikkerhed (ENISA), Europol, Sammenslutningen af Europæiske Tilsynsmyndigheder inden for Elektronisk Kommunikation (BEREC) og EU's Efterretnings- og Situationscenter. Denne værktøjskasse bør tjene som rettesnor for Kommissionen i udviklingen af fælles minimumskrav som yderligere garanti for et højt cybersikkerhedsniveau for 5G-net i hele Unionen.

(25) Med hensyn til foranstaltninger til håndtering af cybersikkerhedsrisici bør det overvejes at øge cybersikkerheden ved at benytte flere forskellige leverandører til etableringen af de enkelte net.

([15]) Europa-Parlamentets og Rådets forordning (EU) 2019/452 af 19. marts 2019 om et regelsæt for screening af udenlandske direkte investeringer i Unionen (EUT L 79 I af 21.3.2019, s. 1).

([16]) Auktionsproceduren vedrørende mindst ét frekvensbånd forventes gennemført i 2019 i 11 medlemsstater: Belgien, Frankrig, Grækenland, Irland, Litauen Nederlandene, Portugal, Tjekkiet, Tyskland, Ungarn og Østrig. Der er i 2020 planlagt seks auktioner mere i følgende medlemsstater: Det Forenede Kongerige Litauen (forskellige frekvenser), Malta, Polen Slovakiet og Spanien. Kilde: http://5gobservatory.eu/observatory-overview/observatory-reports/.

(26) Denne henstilling bør ikke berøre medlemsstaternes beføjelser med hensyn til aktiviteter vedrørende offentlig sikkerhed, forsvar, statens sikkerhed og statens aktiviteter på det strafferetlige område, herunder medlemsstaternes ret til at udelukke tjenesteudbydere eller leverandører fra deres markeder af hensyn til den nationale sikkerhed.

VEDTAGET DENNE HENSTILLING:

I. **MÅL**

1. Med henblik på at bidrage til udviklingen af en EU-tilgang til sikring af cybersikkerheden i forbindelse med 5G-net udpeger denne henstilling de tiltag, der bør træffes for, at:

   a) medlemsstaterne kan vurdere de cybersikkerhedsrisici, der påvirker 5G-net på nationalt plan, og træffe de nødvendige sikkerhedsforanstaltninger

   b) medlemsstaterne og de relevante EU-institutioner, EU-agenturer og andre EU-organer i fællesskab kan udarbejde en koordineret EU-risikovurdering på grundlag af den nationale risikovurdering

   c) den samarbejdsgruppe, der er nedsat ved direktiv (EU) 2016/1148 (samarbejdsgruppen) kan fastlægge et eventuelt fælles sæt foranstaltninger, der skal træffes for at afbøde de cybersikkerhedsrisici, som er forbundet med infrastrukturer, der understøtter det digitale økosystem, navnlig 5G-net.

II. **DEFINITIONER**

2. I denne henstilling forstås ved:

   a) »5G-net«: et sæt af alle relevante netinfrastrukturelementer for mobil og trådløs kommunikationsteknologi, som anvendes til at skabe konnektivitet og værdiforøgende tjenester, med højydelsesegenskaber såsom meget høj datahastighed og -kapacitet, kommunikation med lav latenstid, ultrahøj pålidelighed og understøttelse af et stort antal forbundne enheder. Disse kan omfatte gamle netelementer baseret på tidligere generationer af mobil og trådløs kommunikationsteknologi såsom 4G eller 3G. 5G-net bør anses for at omfatte alle relevante dele af nettet.

   b) »infrastrukturer, der understøtter det digitale økosystem«: infrastrukturer, der anvendes til digitalisering af en lang række kritiske anvendelser i vores økonomi og samfund.

III. **TILTAG PÅ NATIONALT PLAN**

3. Medlemsstaterne bør senest den 30. juni 2019 foretage en risikovurdering af 5G-infrastrukturen og herunder fastlægge de mest følsomme elementer, hvor sikkerhedsbrud ville have betydelige negative konsekvenser. Inden for samme frist bør medlemsstaterne også gennemgå sikkerhedskravene og de gældende risikohåndterringsmetoder på nationalt plan for at tage højde for de cybertrusler, der kan opstå i forbindelse med i) tekniske faktorer, såsom 5G-nettets specifikke tekniske egenskaber, og ii) andre faktorer som f.eks. den retlige og politiske ramme, som leverandører af informations- og kommunikationsteknologiudstyr kan være underlagt i tredjelande.

4. På grundlag af denne nationale risikovurdering og evaluering og under hensyntagen til den igangværende koordinerede indsats på EU-plan bør medlemsstaterne:

   a) opdatere sikkerhedskravene og de anvendte risikohåndterringsmetoder i forbindelse med 5G-net

   b) ajourføre de relevante forpligtelser, der pålægges virksomheder, som udbyder offentlige kommunikationsnet eller offentligt tilgængelige elektroniske kommunikationstjenester i medfør af artikel 13a og 13b i direktiv 2002/21/EF

   c) knytte vilkår vedrørende sikring af offentlige net mod uautoriseret adgang til den generelle tilladelse og anmode de virksomheder, der deltager i eventuelle kommende procedurer for tildeling af brugsret til radiofrekvenser i 5G-frekvensbånd, forpligte sig til at opfylde sikkerhedskravene i forbindelse med net i direktiv 2002/20/EF

   d) anvende andre forebyggende foranstaltninger, der tager sigte på at afbøde potentielle cybersikkerhedsrisici.

5. De i punkt 4 omhandlede foranstaltninger bør omfatte strengere forpligtelser for leverandører og operatører til at holde de følsomme dele af nettene sikre samt forpligtelser til, hvor det er relevant, at give de kompetente nationale myndigheder adgang til relevante oplysninger om planlagte ændringer i elektroniske kommunikationsnet samt krav om specifikke informationsteknologikomponenter og -systemer, hvis sikkerhed og integritet på forhånd er afprøvet af de nationale kontrol-/certificeringslaboratorier.

6. To eller flere medlemsstater bør gennemføre fælles sikkerhedsevalueringer, hvor de anvender og deler den passende tekniske ekspertise og de passende tekniske faciliteter vedrørende infrastrukturer, der understøtter det digitale økosystem og 5G-net, når f.eks. den samme virksomhed er aktiv eller anlægger netinfrastruktur i mere end én medlemsstat, eller hvis der er betydelige ligheder i netstrukturen. Det Europæiske Agentur for Cybersikkerhed (ENISA), Europol og Sammenslutningen af Europæiske Tilsynsmyndigheder inden for Elektronisk Kommunikation (BEREC) bør prioritere anmodninger fra medlemsstaterne om støtte hertil. Resultaterne af disse evalueringer bør sendes til samarbejdsgruppen og netværket af enheder, der håndterer IT-sikkerhedshændelser.

IV. **KOORDINERET INDSATS PÅ EU-PLAN**

7. For at udvikle en fælles tilgang til håndtering af cybersikkerhedsrisiciene i 5G-net bør medlemsstaterne senest den 30. april 2019 indføre et særligt arbejdsforløb i samarbejdsgruppen. Medlemsstaterne bør invitere de relevante myndigheder til at deltage i samarbejdsgruppens arbejde, når det findes hensigtsmæssigt.

En koordineret europæisk risikovurdering

8. Medlemsstaterne bør udveksle oplysninger med hinanden og med de relevante EU-organer for at skabe en fælles bevidsthed om de eksisterende og potentielle cybersikkerhedsrisici i 5G-net.

9. Medlemsstaterne bør senest den 15. juli 2019 sende deres nationale risikovurderinger til Kommissionen og til Det Europæiske Agentur for Cybersikkerhed (ENISA).

10. Det Europæiske Agentur for Cybersikkerhed (ENISA) bør udfærdige en konkret kortlægning af trusselsbilledet vedrørende 5G-net. Samarbejdsgruppen og netværket af enheder, der håndterer IT-sikkerhedshændelser, som er oprettet ved direktiv (EU) 2016/1148, bør støtte denne proces.

11. Med støtte fra Kommissionen og sammen med Det Europæiske Agentur for Cybersikkerhed (ENISA) bør medlemsstaterne under hensyntagen til alle disse forhold og senest den 1. oktober 2019 foretage en fælles evaluering af eksponeringen på EU-plan med hensyn til de risici, der er forbundet med infrastrukturer, som understøtter det digitale økosystem, navnlig 5G-net.

12. I den fælles evaluering bør der lægges vægt på at analysere risiciene for de særligt følsomme eller sårbare elementer i 5G-nettets centrale dele, for drifts- og vedligeholdelsescentre samt for de 5G-accessnetelementer, som anvendes til industrielle applikationer.

13. I anden fase bør denne fælles evaluering udvides til at omfatte andre strategiske dele af den digitale værdikæde.

En fælles EU-værktøjskasse til håndtering af risiciene

14. Samarbejdsgruppen bør i sit arbejde indkredse god praksis blandt de nationale foranstaltninger af den type, der omhandles i punkt 4. På grundlag af de nationale eksempler på god praksis bør der senest den 31. december 2019 opnås enighed om en værktøjskasse, der med passende, effektive og forholdsmæssige risikohåndterringsforanstaltninger til afbødning af de udpegede cybersikkerhedsrisici på nationalt plan og EU-plan kan tjene som rettesnor for Kommissionen i udviklingen af fælles minimumskrav som yderligere garanti for et højt cybersikkerhedsniveau for 5G-net i hele Unionen.

15. Værktøjskassen bør omfatte:

a) en fortegnelse over de typer sikkerhedsrisici, der kan påvirke cybersikkerheden i forbindelse med 5G-net (f. eks. risici vedrørende forsyningskæden, sårbart software, adgangskontrol, den retlige og politiske ramme, som leverandører af informations- og kommunikationsteknologiudstyr kan være underlagt i tredjelande), samt

b) en række mulige afhjælpende foranstaltninger (f.eks. certificering foretaget af en uafhængig tredjepart vedrørende hardware, software eller tjenester, formel afprøvning af hardware og software eller overensstemmelseskontrol, procedurer, der sikrer gennemførelse og håndhævelse af adgangskontrol, indkredsning af produkter, tjenester eller leverandører, der betragtes som potentielt ikke-sikre osv.). Foranstaltningerne bør omfatte alle typer sikkerhedsrisici, der efter risikovurderingen er blevet påpeget i en eller flere medlemsstater.

16. Når der er opstillet europæiske cybersikkerhedscertificeringsordninger vedrørende 5G-net, bør medlemsstaterne i overensstemmelse med EU-retten vedtage nationale tekniske forskrifter, der foreskriver obligatorisk certificering af de informations- og kommunikationsteknologiske produkter, tjenester eller systemer, der omfattes af disse ordninger.

17. Medlemsstaterne bør sammen med Kommissionen fastlægge de vilkår vedrørende sikring af offentlige net mod uautoriseret adgang, der skal tilknyttes den generelle tilladelse, og sikkerhedskrav i forbindelse med net med henblik på at anmode om tilsagn fra de virksomheder, der deltager i procedurer for tildeling af brugsret til radiofrekvenser i 5G-frekvensbånd i henhold til direktiv 2002/20/EF. Disse bør, hvis det er muligt, afspejles i foranstaltningerne i punkt 4, litra c).

18. Medlemsstaterne bør samarbejde med Kommissionen om at udarbejde særlige sikkerhedskrav, der kan finde anvendelse ved offentlige indkøb i forbindelse med 5G-net. Heri bør indgå obligatoriske krav om at indføre cybersikkerhedscertificeringsordninger i forbindelse med offentlige udbud, for så vidt sådanne ordninger endnu ikke er bindende for alle leverandører og operatører.

V. **EVALUERING**

19. Medlemsstaterne bør samarbejde med Kommissionen om senest den 1. oktober 2020 at vurdere virkningerne af denne henstilling med henblik på at fastlægge hensigtsmæssige fremgangsmåder. I denne vurdering bør der tages højde for resultatet af den koordinerede EU-risikovurdering og EU-værktøjskassen.

Udfærdiget i Strasbourg, den 26. marts 2019.

På Kommissionens vegne

Julian KING

Medlem af Kommissionen