Digitaliserings-
styrelsen

Høringsnotat

14. maj 2025
KDRT/SEBYVI og JULCHR
J. nr. 2024-13336

Høringsnotat over høringssvar om bekendtgørelse om validering, verifikation og udlevering af domænenavnsregistreringsdata

1. Høringen

Høringsperiode:
Udkastet til bekendtgørelse om validering, verifikation og udlevering af domænenavnsregistreringsdata har fra den 26. marts 2025 til den 29. april 2025 været sendt i høring hos en række myndigheder, organisationer m.v. Udkastet blev den 27. marts 2025 endvidere sendt til Udvalget for Digitalisering og It til orientering. Herudover blev udkastet til bekendtgørelsen, høringsbrev og høringsliste offentliggjort på Høringsportalen den 26. marts 2025.

Hørte myndigheder og organisationer m.v.:
Der er modtaget 11 høringssvar fra de hørte myndigheder og organisationer, heraf ni med bemærkninger. Nedenfor i tabel 1 følger en alfabetisk oversigt over hørte myndigheder, organisationer m.v. Ud for hver høringspart er det ved afkrydsning angivet, om der er modtaget høringssvar, og om høringsparten i givet fald har haft bemærkninger til bekendtgørelsesudkastet. Oversigten omfatter herudover interessenter, som ikke er blandt de hørte myndigheder, organisationer m.v., men som på egen foranledning har sendt bemærkninger. Sådanne interessenter er i oversigten markeret med *.

Tabel 1: Oversigt over eksterne høringsparter og afgivne høringssvar

Høringspart	Høringssvar modtaget	Bemærk-ninger	Ingen bemærk-ninger	Ønsker ikke at afgive hørings-svar
Christian Schmidt*	X	X		
Dansk Erhverv	X	X		
Dansk Arbejdsgiverforening	X			X
Dansk Industri (DI)	X	X		
Dansk Internet Forum (DIFO)	X	X		
Dataetisk Råd	X			X
Datatilsynet	X		X	

Internetaktører[1]	X	X		
Norid*	X	X		
One Registry	X	X		
Rettighedsalliancen	X	X		
Stiftelsen for Internetinfrastruktur (Internetstiftelsen)*	X	X		
Aarhus Universitet	X		X	

2. Høringssvarene

Nedenfor er gengivet de væsentligste punkter i de modtagne høringssvar. Digitaliseringsstyrelsens bemærkninger til høringssvarene, herunder om der er foretaget ændringer i anledning af høringssvarene, er skrevet med kursiv. Under pkt. 3 er det opsummeret, hvilke ændringer der er foretaget i forhold til det udkast, som har været i offentlig høring.

Samtlige høringssvar, der indeholder indholdsmæssige ændringer, er vedlagt særskilt.

2.1 Generelle bemærkninger til bekendtgørelsen:

DI, Internetstiftelsen, Dansk Erhverv, DIFO, One Registry, Norid og Internetaktørerne angiver, at bekendtgørelsen i sin nuværende form fraviger minimumsimplementeringen, som er nævnt i NIS 2-loven og udgør en overimplementering af NIS 2-direktivet. Flere nævner i den forbindelse, at bekendtgørelsen medfører betydelige ekstra byrder og omkostninger for borgere og erhvervslivet, risiko for suspendering eller sletning af domænenavne, risiko for dårligere cybersikkerhed, og at det bliver mindre attraktivt at anvende .dk domænenavne. Derudover nævnes også, at Danmark for nu er det eneste EU-land, der pålægger så omfattende verifikationskrav. Flere opfordrer til, at bekendtgørelsen justeres, så den er mere risikobaseret, proportional og driftsnær ift. at sikre cybersikkerhed uden at skabe uforholdsmæssige byrder eller sårbarheder for danske virksomheder.

DIFO og Norid understreger, at danske virksomheder pålægges flere administrative byrder end andre europæiske virksomheder, som vil skabe ulige konkurrencevilkår på det europæiske marked. **One Registry** anfører, at man hverken teknisk eller kontraktuelt vil kunne opfylde kravene i bekendtgørelsen. Det skyldes bl.a., at det er forhandlere, der har den direkte relation til

[1] Høringssvar fra mere end 60 nationale og internationale internetsamfundsaktører. For en fuld liste henvises til bilaget over de modtagne høringssvar

registranterne, og at verifikationssystem vil kunne komme i konflikt med forhandlernes processer. Det kan føre til uønsket suspension af hjemmesider.

Digitaliseringsstyrelsens kommentarer:
Med hensyn til spørgsmålet om, hvorvidt udkastet til bekendtgørelsen udgør en overimplementering af NIS 2-direktivet skal Digitaliseringsstyrelsen bemærke, at bekendtgørelsesudkastet i vidt omfang følger de retningslinjer, som NIS 2-samarbejdsgruppen har udstedt, jf. Recommendations for the implementation of NIS2 Directive Article 28 (Database of domain name registration data) - Final Version, September 2024. Det fremgår eksplicit af retningslinjerne, at disse "are to be considered as minimum requirements that the Member States are recommended to include in their transposition laws to fulfil the objectives of Article 28 of the NIS2 Directive". NIS 2-samarbejdsgruppen, som består af alle EU-medlemsstaterne, har således tiltrådt, at retningslinjerne indebærer en minimumsimplementering af NIS 2-direktivets artikel 28. Derudover er det i bemærkningerne til § 11, stk. 8, i NIS 2-loven forudsat, at administrative forskrifter kan udstedes på baggrund af retningslinjer fra bl.a. NIS 2-samarbejdsgruppen.

Retningslinjerne er ikke juridisk bindende for medlemsstaterne, men da de er udtryk for minimumsimplementering, er det Digitaliseringsstyrelsen vurdering, at der alene er et begrænset råderum i forhold til at lempe kravene i den nationale implementering.

Det er Digitaliseringsstyrelsens samlede vurdering, at udkastet til bekendtgørelsen, som den blev sendt i høring, ikke generelt er udtryk for overimplementering. På baggrund af de modtagne høringssvar har styrelsen imidlertid fundet grundlag for at ændre bekendtgørelsen på en række punkter.

2.2 Bemærkninger til de enkelte bestemmelser

2.2.1 Krav om validering og verifikation af både e-mailadresse og telefonnummer (§ 3, stk. 1):

DI, Internetstiftelsen, Dansk Erhverv, DIFO, Norid, One Registry og internetaktørerne anfører, at der alene bør kræves én kontaktmetode, og at det ikke er i overensstemmelse med NIS 2-loven, direktivets betragtninger og ICANN-standarder, at bekendtgørelsen kræver verifikation af både e-mail og telefonnummer. Flere nævner i den forbindelse, at direktivets præambelbetragtning 111 lægger op til, at verifikation af én kontaktmåde er tilstrækkeligt.

DIFO bemærker, at kravet i § 3, stk. 1, går ud over minimumsimplementeringen. Samtidig er der i domæneloven et krav om at sikre retvisende oplysninger om postadresse for .dk-domænenavne. Der vil dermed være krav om verifikationer

af tre forskellige kontaktmåder, hvilket må anses at gå udover, hvad der er nødvendigt for at opfylde formålet med NIS 2-lovforslagets § 11.

Internetaktørerne fremhæver, at bekendtgørelsen vil gøre danske forhandlere til de eneste i verden, i det mindste under den nuværende implementering af NIS 2 i EU, der kræver, at registranter verificerer både deres e-mailadresse og telefonnummer, når de registrerer et domænenavn. Dette vil øge kompleksiteten, skabe friktion i kunderejsen og medføre betydelige omkostninger, som i praksis vil føre til højere priser for registranterne. Dette kan få registranter til at vælge ikke-danske forhandlere for at undgå denne ekstra byrde.

Internetstiftelsen, DI, Dansk Erhverv, DIFO og Norid fremhæver, at der bør gives metodefrihed i, hvordan operationel verifikation gennemføres. DIFO og Norid anfører, at de foreslåede regler kan hindre allerede velfungerende verifikationsmetoder samt besværliggøre, eller måske endda umuliggøre, fremtidige bedre verifikationsmetoder herunder henset til, at artikel 28 i NIS 2-direktivet er formuleret på en teknologineutral måde.

Digitaliseringsstyrelsens kommentarer:
Digitaliseringsstyrelsen skal indledningsvis bemærke, at NIS 2-direktivets artikel 28 – og dermed den danske implementering heraf – fastsætter bestemmelser om, at der skal føres en særskilt database, som indeholder nøjagtige og fuldstændige domænenavnsregistreringsdata, bl.a. vedrørende angivelse af registrantens e-mailadresse og telefonnummer. NIS 2-direktivet fastsætter endvidere krav om, at disse kontaktoplysninger skal være nøjagtige og fuldstændige.

Det fremgår i den forbindelse af NIS 2-direktivets betragtning 111, at mindst én kontaktmåde bør verificeres. NIS 2-arbejdsgruppen har imidlertid anbefalet, at såvel telefonnummer som e-mailadresse verificeres.

Det er Digitaliseringsstyrelsens opfattelse, at der ved vurderingen af, hvorvidt der bør ske verificering af én eller begge kontaktoplysninger, bør foretages en samlet afvejning af, om det vil være muligt at komme i kontakt med de pågældende registranter i tilfælde, hvor dette er påkrævet – også med kort varsel. Verificeringer af kontaktoplysninger vil efter styrelsens opfattelse alt andet lige styrke visheden for, at registranter i praksis er kontaktbare. Styrelsen vil imidlertid ikke udelukke, at topdomænenavneadministratorerne og enheder, der leverer domænenavnsregistreringstjenester på anden vis vil kunne sikre, at såvel e-mailadresser som telefonnumre til stadighed er nøjagtige og fuldstændige.

På baggrund af de modtagne høringssvar lægger Digitaliseringsstyrelsen op til, at kravet om verifikation af både e-mail og telefonnummer lempes, således at

der kun kræves verifikation af én af de to kontaktmuligheder. Konsekvensen heraf er, at det vil være op til den enkelte enhed på anden vis at sikre, at den kontaktoplysning, som ikke efter bekendtgørelsens krav valideres og verificeres, til stadighed er nøjagtig og fuldstændig.

2.2.2 Krav om validering og verifikation ved fornyelse eller årlig bekræftelse (§ 3, stk. 1, og § 3, stk. 5)

Internetstiftelsen, One Registry, Dansk Erhverv og Internetaktørerne anfører, at validering og verifikation ved fornyelser vil være en for vidtgående regulering. Flere peger på, at kravet i bekendtgørelsen forventes at ville medføre deaktivering/suspendering af legitime domæner med korrekte ejeroplysninger. Dette vil udgøre en risiko for cybersikkerheden og stabiliteten på internettet.

Internetaktører og One Registry foreslår, at der kun kræves verifikation ved registrering, ved ændring af relevante datafelter, eller når der er en begrundet årsag til at betvivle nøjagtigheden af de registrerede oplysninger.

DI, Internetstiftelsen, DIFO, Dansk Erhverv og Internetaktører fremhæver, at der er forretningskritiske og sikkerhedsmæssige konsekvenser forbundet med en årlig bekræftelse af kontaktoplysninger. Høringsparterne anfører, at kravet om, at en indehaver skal bekræfte e-mail og telefonnummer (aktivt svar) er for vidtgående og vil medføre, at et stort antal aktive domæner deaktiveres eller slettes, hvilket kan medføre en sikkerhedsrisiko. **DI** anbefaler i den forbindelse, at der laves en differentieret tilgang afhængig af, om domænet anvendes til teknisk eller infrastrukturel brug, indførelse af karensperioder før sletning af domæner, indførelse af varslinger samt at et domæne ikke bør kunne overgå til en ny registrant inden for en periode, medmindre den tidligere registrant frasiger sig domænet.

DIFO mener, at det er overflødigt, at registranter skal gøre noget aktivt hvert år, når registranten både har gennemført en MitID-kontrol, og oplysningerne er matchet og låst til CPR/CVR-registreret, hvorved navn og adresse opdateres automatisk. **DIFO** foreslår, at der alene stilles krav om, at der foretages en verificering af enten e-mail eller telefonnummer, når kontaktoplysningerne ændres, eller når der i øvrigt er rimelig grund til at tro, at oplysningerne ikke er korrekte.

Digitaliseringsstyrelsens kommentarer:
Som anført overfor lægger Digitaliseringsstyrelsen op til, at kravet om verifikation af både e-mail og telefonnummer lempes for så vidt angår registreringer af domænenavne, således at der kun kræves verifikation af én af de to kontaktmuligheder. For så vidt angår fornyelse af domæner, finder styrelsen – på baggrund af de modtagne høringssvar – endvidere, at krav om verificeringer bør undlades. Styrelsen lægger herved afgørende vægt på det

anførte om, at der er risiko for, at domænenavne suspenderes eller slettes selvom kontaktoplysningerne er korrekte, såfremt registranten ikke reagerer på anmodning om verifikation af oplysningerne ved fornyelse. Konsekvensen heraf er, at det vil være op til den enkelte enhed at etablere procedurer, der til stadighed kan sikre, at e-mailadresser og telefonnumre er nøjagtige og fuldstændige – også ved fornyelser.

2.2.3 Telefonnumre og e-mailadresser skal være formateret i overensstemmelse med standarder (§ 3, stk. 4).

Norid anfører, at kravet til telefonnumres format, kan komme i konflikt med tilgængelighedskrav fastsat i europæisk eller national lovgivning uden for Danmark.

Christian Schmidt foreslår, at henvisningen i § 3, stk. 4, nr. 1. ændres til "RFC 5322 med de ændringer, der følger af RFC 6532", da RFC 5322 bl.a. ikke omfatter bogstaverne Æ, Ø og Å. RFC 6532 udvider syntaksen, så disse tegn kan benyttes både før og efter snabel-a. Christian Schmidt mener, at man bør fremme moderne teknologier, der understøtter det danske sprogs egenart. Dette er især af betydning for personer og virksomheder, hvis navne indeholder et Æ, Ø eller Å, og som naturligt har et ønske om at benytte en e-mailadresse, der afspejler deres rigtige navn.

Digitaliseringsstyrelsens kommentarer:
For så vidt angår NIS 2-samarbejdsgruppens anbefaler til validering af formaterne for telefonnummer og e-mailadresser følger disse ICANN's Registrar Accreditation Agreement (2013). Det følger af NIS 2-direktivets betragtning 111, at procedurer – fx til validering af e-mailadresser og telefonnummer – "bør så vidt muligt tage hensyn til de standarder, der er udviklet af multiinteressent-styringsstrukturerne på internationalt plan", hvilket det her har været muligt at tage hensyn til.

Med hensyn til brug af nye versioner af RFC 5322 fremgår muligheden herfor af NIS 2-samarbejdsgruppens retningslinjer, idet det er angivet, at "Email address should be in the proper format according to RFC 5322 (or its successors)". Det foreslås derfor, at det præciseres i bekendtgørelsen, at RFC 5322 (eller senere standarder, som træder i stedet for) kan anvendes.

2.2.4 Verifikation af en domæneindehaver med flere domænenavne under samme topdomæne (§ 3, stk. 6):

Internetstiftelsen anfører, at det er positivt, at det tillades at genbruge verifikation af en domæneindehaver til flere domæneregistreringer. **Internetstiftelsen, DIFO, One Registry og internetaktører** anfører, at en validering og verifikation af en registrants identitet og kontaktoplysninger skal kunne

genbruges, hvis registranten har registreret flere domænenavne med samme kontaktoplysninger på tværs af forskellige topdomænenavne.

Digitaliseringsstyrelsens kommentarer:
Digitaliseringsstyrelsen skal bemærke, at udkastet til bekendtgørelse i § 3, stk. 6 og § 4, stk. 6 giver mulighed for kun at udføre validering og verificering af en registrants kontaktoplysninger og navn én gang, såfremt registranten har eller vil registrere flere domænenavne under samme topdomænenavn. Hensynet bag bestemmelserne er at undgå at foretage samme validering og verificering flere gange. Det er Digitaliseringsstyrelsens opfattelse, at samme hensyn ligeledes gør sig gældende, hvis en registrant ønsker at registrere flere domænenavne under forskellige topdomænenavne hos én og samme enhed.

På den baggrund lægger Digitaliseringsstyrelsen op til, at bekendtgørelsen ændres, således at verifikation og validering af en registrants kontakt-oplysninger og navn kun skal foretages én gang ved registrering af flere domænenavne hos samme enhed uafhængig af, om domænenavnene er under ét eller flere forskellige topdomænenavne.

2.2.5 Anvendelse af elektronisk identifikation eller risikobaseret tilgang ved registreringer eller fornyelser (§ 4):

Rettighedsalliancen bemærker, at der ikke eksplicit sondres mellem danske og udenlandske registranter. Ifølge de nuværende regler for verifikation anvendes elektronisk identifikation via MitID som udgangspunkt for danske registranter modsat udenlandske, hvor den risikobaserede tilgang anvendes. På den baggrund er der ikke tale om et stærkere grundlag for kontrol i forhold til de nuværende regler, og den risikobaserede tilgang anses ikke som tilstrækkelig for at forhindre misbrug. **Rettighedsalliancen** har konstateret en stigende tendens til, at .dk-domæner anvendes ulovligt, og at disse sider oftest er registreret af udenlandske registranter. På den baggrund foreslås det, at kravene til udenlandske registranter eksplicit skærpes ved, at udenlandske registranter skal opgive ID-dokumentation, og at domænet først aktiveres efter verificering af den udenlandske registrant på linje med danske registranter, der anvender MitID.

Digitaliseringsstyrelsens kommentarer:
Digitaliseringsstyrelsen skal henlede opmærksomheden på, at de nye regler i NIS 2-direktivet om domænenavnsregistreringsdata er rettet mod alle topdomænenavneadministratorer og enheder, der leverer domænenavns-registreringstjenester i EU og ikke kun de nationale topdomænenavne-administratorer såsom .dk.

Det er Digitaliseringsstyrelsens umiddelbare vurdering, at det ikke i denne sammenhæng har været muligt, at fastsætte bestemmelser – på tværs af EU –

om, at validering og verifikation af domænenavnsregistreringsdata skal ske ved brug af elektronisk identifikation, og at NIS 2-samarbejdsgruppen derfor ikke har kunnet fastsætte anbefalinger herom. Det er i forlængelse heraf styrelsens opfattelse, at det i denne sammenhæng vil være uhensigtsmæssigt at fastsætte særskilt nationale regulering for alle topdomænenavne.

2.2.6 Aktivering, suspendering og sletning ved manglende validering eller verifikation af domænenavnsregistreringsdata (§ 5)

Rettighedsalliancen støtter, at et domænenavn først aktiveres, når der er sket verificering af e-mail, telefonnummer og navn med et tilfredsstillende resultat. Samtidig opfordres til, at man udvider bestemmelsen således, at domæner registreret af personer eller virksomheder uden for Danmark suspenderes ved modtagelse af en begrundet anmodning vedrørende mistanke om misbrug, indtil der er foretaget en skærpet kontrol af identifikationsoplysninger.

DIFO og Norid anfører, at det er uforholdsmæssigt byrdefuldt for registranter at få suspenderet og evt. slettet deres domænenavn på grund af en overset verifikation af fx et telefonnummer. **DIFO** anfører, at dette er særlig uhensigtsmæssigt, hvis registranten samtidig har verificeret både sin identitet og e-mailadresse, og for .dk-domænenavne tillige sin postadresse.

Internetaktører påpeger, at det for mange landekodetopdomæner (ccTLDer) ikke er teknisk muligt at sikre, at domæner ikke bliver automatisk aktive ved registrering, og forhandlerne har ingen mulighed for at forsinke aktiveringen. Disse vil dermed ikke kunne leve op til kravet i bekendtgørelsen om, at domænenavne ikke må aktiveres, før registreringsdata er verificeret. Kravet går også videre end det minimum, som NIS 2-direktivet kræver. **Internetaktører** foreslår, at bekendtgørelsen tillader, at verifikationen gennemføres efter registreringen. Dette ville være i overensstemmelse med ICANN RDDS Accuracy Program Specification, som tillader, at verifikationen afsluttes inden for 15 dage efter registrering, overførsel eller dataopdatering. Selv hvis dette krav kun ville gælde, hvor det er teknisk muligt, ville det stadig udgøre en ekstra byrde for danske forhandlere at vedligeholde og drive to forskellige registreringsprocesser parallelt. Det vil i sidste ende være konkurrenceforvridende og stille danske forhandlere ringere end deres udenlandske konkurrenter.

One Registry foreslår, at det tillades, at domæner aktiveres før verifikation, så længe verifikationen gennemføres inden for en rimelig frist.

Digitaliseringsstyrelsens kommentarer:
Høringen har vist, at der er forskellige holdninger til, hvorvidt validering og verifikation bør finde sted før eller efter, at et domænenavn er blevet aktivt. Hensigten med de retningslinjer, som NIS 2-samarbejdsgruppen har fastsat og dermed kravet i bekendtgørelsesudkastet, er at sikre, at der er kendskab til den,

som benytter internettet, således at der vil være mulighed for at efterforske eventuelle ulovligheder, som foregår via internettet fx phising, spredning af malware eller misbrug af børn. Såfremt der først sker en validering og verifikation af en registrant af et domænenavn, efter at domænenavnet er blevet aktivt, vil det være muligt at foretage ulovlige aktiviteter via domænenavnet uden, at der er mulighed for at vide, hvem der står bag aktiviteten og dermed vanskeliggøre eller umuliggøre en efterforskning. Heroverfor står, at det i visse tilfælde ikke er teknisk muligt at foretage en forudgående validering og verifikation af registranten.

På den baggrund lægger Digitaliseringsstyrelsen op til, at der i de situationer, hvor det ikke er teknisk muligt, gives et passende tidsrum til at foretage den nødvendige validering og verifikation af registranten. I høringen er foreslået 15 dage, hvilket styrelsen imidlertid vurderer at være meget lang tid med dertil hørende øget risiko for, at der udføres ulovlige aktiviteter via domænenavnet, uden at der er reel mulighed for at kunne efterforske ulovlighederne. På den baggrund foreslås det, at der i de tilfælde, hvor det ikke er teknisk muligt at foretage en validering og verifikation af registranten før domænenavnet gøres aktivt, skal foretages validering og verifikation af registranten, senest 72 timer efter domænenavnet er blevet aktivt. Hvis en validering og verifikation af registranten ikke kan ske med et tilfredsstillende resultat inden for de 72 timer, vil domænenavnet skulle suspenderes uden unødigt ophold.

2.2.7 Adgang til domæneregistreringsdata (§ 6)

DI, Dansk Erhverv, DIFO og Norid fremhæver, at 24-timersfristen for hasteanmodninger går videre end det der kræves i NIS 2-direktivet. **DI og DIFO** nævner i den forbindelse, at det skaber praktiske og retlige problemer, især for virksomheder uden døgnbemanding. **DI** fremhæver at en bedre balance ville kunne opnås med en frist på 72 timer – med mulighed for forkortelse i særligt alvorlige tilfælde. **DIFO** anfører, at det er betænkeligt, at der i bemærkningerne til § 11, stk. 8, i NIS 2-loven efter høringsperioden er indsat et afsnit, der nævner at administrative forskrifter kan udstedes på baggrund af retningslinjer udarbejdet af bl.a. samarbejdsgruppen. **DIFO** fremhæver hertil, at der ikke fremgår nogen 24 timers frist i § 11, stk. 5, og at det er betænkeligt, at det alene er i lovbemærkningerne, at det er fastsat, at man kan fastsætte tidsrammer for udlevering af oplysninger ved hasteanmodninger.

Internetaktører påpeger, at bekendtgørelsen ikke indeholder bestemmelser, der sikrer en afbalancering af borgerens grundlæggende ret til privatlivets fred og databeskyttelse med behovet for effektiv retsforfølgelse af strafbare handlinger. Internetaktører foreslår, at der udarbejdes bestemmelser i lighed med E-evidensforordningens regler om anmodninger om oplysninger, da forordningens anvendelsesområde vil overlappe med NIS 2. Dette vil mindske risikoen for

lovkonflikter og samtidigt sikre, at vurderingen af en anmodnings legitimitet sker under hensyntagen til alle de grundlæggende rettigheder og interesser.

One Registry påpeger, at der bør indføres klare, proportionalitetsbaserede regler for udlevering af registreringsdata til tredjepart.

Rettighedsalliancen har angivet, at man støtter § 6, som sikrer at der gives adgang til specifikke registreringsdata inden for 72 timer efter en begrundet anmodning fra en legitim adgangssøger.

Digitaliseringsstyrelsens kommentarer:
For så vidt angår spørgsmålet om hasteanmodninger anføres der i høringssvarene, at fristen for besvarelse af anmodninger om udlevering af domænenavsregistreringsdata bør være 72 timer med mulighed for forkortelse i særlig alvorlige tilfælde. Digitaliseringsstyrelsen har fjernet bestemmelsen vedr. hasteanmodninger på baggrund af de modtagne høringssvar.

2.2.8 Legitime adgangssøgende (§ 6)

DIFO og One Registry anfører, at bekendtgørelsen ikke giver yderligere vejledning i forhold til loven for så vidt angår, hvem der kan anses at være legitime adgangssøgende. Der er nærmere efterspurgt retningslinjer for, hvordan det kan afklares, hvorvidt fysiske og juridiske personer uden for Danmark er legitime adgangssøgende, og hvordan det kan afgøres, om de har saglige grunde til at få udleveret de ønskede oplysninger. **DIFO** har derudover også anført, at indførelsen af hjemmel til at udlevere oplysninger til "øvrige adgangssøgende" i bekendtgørelsens § 6 stk. 3, er problematisk, da det alene er beskrevet i bemærkningerne til NIS 2-loven og ikke i lovteksten. På grund af mangel på direkte lovhjemmel foreslår DIFO, at § 6, stk. 3, udgår.

Digitaliseringsstyrelsens kommentarer:
For så vidt angår spørgsmålet om yderligere vejledning i forhold til, hvem der kan anses for at være legitime adgangssøgende, skal Digitaliseringsstyrelsen henvise til, at det fremgår af NIS 2-direktivets præambelbetragtning 110, at der ved legitime adgangssøgende forstås enhver fysisk eller juridisk person, der fremsætter en anmodning i henhold til EU-retten eller national ret. Styrelsen kan i den forbindelse oplyse, at der i regi af NIS 2-samarbejdsgruppen søges afdækket, hvilke konkrete fysiske eller juridiske personer, som i EU er legitime adgangssøgende i henhold til NIS 2-direktivet. Kommissionen har i den forbindelse oplyst vedrørende "legitime adgangssøgende", at der ikke gælder et krav om gensidig anderkendelse af andre landes legitime adgangssøgere. På den baggrund justeres definitionen af "legitime adgangssøgende" i bekendtgørelsen, således at andre EU-medlemsstater legitime adgangssøgende ikke automatisk anses at være legitime adgangssøgende i Danmark.

Digitaliseringsstyrelsen bemærker, at bekendtgørelsens § 6, stk. 3, ikke indebærer, at der skal udleveres oplysninger til "øvrige adgangssøgende". Bestemmelsen sikrer alene, at der skal gives besked om, hvorvidt en anmodning om oplysninger imødekommes eller afslås.

2.2.9 Ikrafttrædelsesdato (§ 9)

DIFO har anmodet om, at bekendtgørelsens ikrafttrædelsesdato udskydes til den 1. januar 2026, så der er tilstrækkelig tid til at tilpasse forretningsprocesser og it-systemer til kravene i bekendtgørelsen.

Digitaliseringsstyrelsens *kommentarer:*
Digitaliseringsstyrelsen er opmærksom på, at bekendtgørelsen i et vist omfang fastsætter bestemmelser, som forudsætter en ikke ubetydelig implementering i praksis. På den baggrund finder styrelsen, at bekendtgørelsens ikrafttrædelsesdato udskydes til den 1. januar 2026. Styrelsen skal for en god ordens skyld bemærke, at NIS 2-lovens krav, herunder kravene som fastsat i § 11, træder i kraft med lovens ikrafttræden.

3. Sammenfatning af ændringer i bekendtgørelsen efter høringen

Ændringer til bekendtgørelsen:

1. Lempe krav om validering af både e-mail og telefon ved registrering, så det er tilstrækkeligt, at det alene er én af de to kontaktmuligheder, der skal valideres (§ 3, stk.1 samt konsekvensrettelser)
2. Fjerne kravet om validering ved fornyelse (§ 3, stk. 1 og stk. 5, samt § 5, stk. 2)
3. Det præciseres ift. anvendelsen af e-mail formatet RFC 5322, at også fremtidige formater, der afløser RFC 5322 kan anvendes (§ 3, stk. 4).
4. Justering så verificering og validering af en registrant (navn og kontaktoplysninger) der har flere domænenavne hos samme enhed, kun skal foretages én gang hos samme enhed (§ 3, stk. 6 og § 4, stk.6).
5. Der indføres en undtagelse til kravet om ikke at aktivere et domænenavn før validering er sket. Således vil et domænenavn kunne gøres aktivt i 72 timer, i tilfælde hvor det ikke teknisk er muligt at validere og verificere domænenavnet før det gøres aktivt, og under forudsætning af, at der inden for den tidsperiode foretages tilfredsstillende validering og verifikation. Sker dette ikke skal domænenavnet suspenderes eller slettes uden ugrundet ophold (ny § 5, stk. 2).
6. *Definitionen af "legitime adgangssøgende" i bekendtgørelsen justeres, således at andre EU-medlemsstater legitime adgangssøgende ikke*

automatisk anses at være legitime adgangssøgende i Danmark. Derfor udgår "i en af EU's medlemsstater".

7. Bestemmelserne vedr. hasteanmodninger i bekendtgørelsens § 2, litra 8, § 6, stk. 1, og § 6, stk. 2, er taget ud af bekendtgørelsen.
8. Der er derudover foretaget mindre ændringer af sproglig, redaktionel og lovteknisk karakter.