

DIGST-NIS2

Fra: -----
Sendt: 6. april 2025 12:13
Til: DIGST-NIS2
Emne: Høring over bekendtgørelse om validering, verifikation og udlevering af domænenavnsregistreringsdata

[EKSTERN E-MAIL] Denne e-mail er sendt fra en ekstern afsender.

Vær opmærksom på, at den kan indeholde links og vedhæftede filer, som ikke er sikre.

Hermed en bemærkning til udkast til bekendtgørelse om validering, verifikation og udlevering af domænenavnsregistreringsdata.

I bekendtgørelsen henvises til RFC 5322. Jeg foreslår, at denne henvisning ændres til "RFC 5322 med de ændringer, der følger af RFC 6532".

Iflg. RFC 5322 består en e-mailadresse udelukkende af tegn fra ASCII-tegnsættet, hvilket ikke omfatter bl.a. Æ, Ø og Å. RFC 6532 udvider syntaksen, så disse tegn kan benyttes både før og efter snabel-a, eksempelvis rådhuset@københavn.dk.

RFC 6532 blev udgivet i 2012. Efter en sløv start er standarden i dag understøttet såvel af populære mailservere (eksempelvis Microsoft Exchange og Postfix) som af de største skybaserede e-mailtjenester (Microsoft 365 og Google Apps).

Der er givetvis stadig nogen, som benytter utidssvarende e-mailsystemer, der ikke understøtter RFC 6532. Jeg mener dog ikke, at man med bekendtgørelsen bør tage særhensyn til disse. Tværtimod bør man 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.

Med venlig hilsen

Digitaliseringsstyrelsen
NIS2@digst.dk

Den 28. april 2025

Høringssvar til udkast til bekendtgørelsen om validering, verifikation og udlevering af domænenavnregistreringsdata

Generelle bemærkninger

Dansk Erhverv takker for muligheden for at komme med kommentarer til udkast til bekendtgørelsen om validering, verifikation og udlevering af domænenavnsregistreringsdata.

Dansk Erhverv bakker op om det overordnede formål med NIS2 nemlig at styrke cybersikkerheden i Danmark. Samtidig er Dansk Erhverv dog bekymrede for, at den forslåede bekendtgørelse på en række punkter – herunder i relation til verificeringer af e-mailadresse og telefonnummer - udgør overimplementering af NIS2-direktivet på trods af, at der gentagne gange i den danske NIS 2 lov er anført, at loven foretager en minimumsimplicitering og skal fortolkes i overensstemmelse med NIS 2- direktivet.

Opretholdes overimplementeringen, vil det medføre betydelige ekstra byrder og omkostninger for erhvervslivet og borgere, som vil skulle gennemføre uforholdsmæssige mange verificeringer af deres e-mailadresse og telefonnummer med den konsekvens, at deres domænenavn suspenderes, hvis verificeringen ikke gennemføres.

Dansk Erhverv er bekymrede for, at en del danske virksomheder vil finde, at der er for store forretningsmæssige risici ved at basere sin forretning på et .dk-domænenavn, hvis der indføres den omfattende risiko for, at domænenavnet suspenderes.

.dk-domænenavne har en meget høj grad af sikkerhed sammenlignet med andre domænenavnsendelser. Fravælges .dk-domænenavne til fordel for andre mere usikre domænenavnsendelser, vil det medføre en lavere grad af sikkerhed for danske virksomheder, der bl. a. anvender domænenavnet til deres hjemmeside og e-mailservice.

Specifikke bemærkninger

Vedr. tidspunkter for validering og verificering af e-mailadresse og telefonnummer (§ 3):

Dansk Erhverv bemærker, at bekendtgørelsen stiller krav om verificering ved registrering og fornyelse af et domænenavn.

Dette er meget rigtigt og byrdefuldt taget i betragtning, at der er ca. 1.3 mio .dk-domænenavne, der vil være omfattet heraf. Hertil kommer andre domænenavnsendelser såsom .nu og .com. Det giver heller ikke den passende og dynamiske metodefrihed for dem, der skal både igangsætte og gennemføre verificeringerne.

Vedr. kravet om validering og verificering af både e-mailadresse og telefonnummer (§ 3):

Dansk Erhverv bemærker, at kravet om validering og verificering af både e-mailadresse og telefonnummer går imod såvel lovbemærkningerne til NIS2-lovens § 11, stk. 3, NIS2-direktivets betragtning 111 og til ICANN's standarder.

Samtidig bemærkes det, at der fra lovgivers side er tilkendegivet, at man kun behøver at verificere mindst én kontaktmåde for registranten.

Vedr. hvordan verificering af e-mailadresse og telefonnummer skal ske:

Dansk Erhverv bemærker, at det er uklart i bekendtgørelsen, hvad der konkret kræves ifm. en verificering af e-mailadresse og telefonnummer.

§ 3, stk. 1, henviser til en operationel verificering; altså en sikring af, at kontaktoplysningerne er funktionelle og muliggør kontakt. Samtidig ses i § 3, stk. 5, i sager om fornyelse et krav om, at registranten bekræfter sin e-mailadresse og sit telefonnummer – altså et krav om aktiv respons. Aktiv respons er uhjemlet og vil medføre et uforholdsmæssigt stort antal suspensioner, hvor registranter overser, at de skal reagere aktivt eller undlader at gøre dette af frygt for, at der er tale om phishing og lign.

Vedr. udlevering af domænenavnsregistreringsdata (§ 6):

Dansk Erhverv bemærker, at der i bekendtgørelsen er indført et krav om udlevering af oplysninger inden for 24 timer, hvis der er tale om en hasteanmodning fra en legitim adgangssøgende, og at dette – som anerkendt i Digitaliseringsstyrelsens høringsbrev – går videre end en minimumsimplementering af NIS2-direktivet.

Med venlig hilsen

Frederikke Rosendal Egede Saabye

Fagchef for digitalisering, Dansk Erhverv

Digitaliseringsstyrelsen
Att.: Kontor for digital regulering og tilsyn
Landgreven 4
1017 København K
nis2@digst.dk

Validering, verifikation og udlevering af domænenavnsregistreringsdata

Dansk Industri(DI) takker for muligheden for at afgive høringssvar. Som repræsentant for en bred kreds af danske virksomheder vil vi gerne sætte fokus på de erhvervsmæssige og sikkerhedsmæssige konsekvenser af den foreslåede bekendtgørelse – særligt de områder, hvor kravene går videre end det bagvedliggende NIS2-direktiv tilsiger.

Overimplementering og risiko for fravalg af .dk

Dansk Industri finder, at bekendtgørelsen i sin nuværende form udgør en overimplementering af NIS2-direktivet. Det gælder særligt i relation til krav om verifikation ved både registrering og fornyelse, samt kravet om verifikation af både e-mailadresse og telefonnummer. Denne overimplementering risikerer at gøre det mindre attraktivt at anvende .dk-domæner eller danske registratorer, hvilket svækker både den danske digitale infrastruktur og tilliden til .dk som sikker topdomænezone.

Forretningskritiske og sikkerhedsmæssige konsekvenser af § 3, stk. 5

DI finder anledning til at fremhæve væsentlige problematikker forbundet med kravet om årlig bekræftelse af kontaktoplysninger:

1. Forretningskritiske konsekvenser ved fejl og misforståelser

Kravet indebærer en risiko for, at domæner utilsigtet suspenderes eller slettes, fx som følge af administrative fejl eller manglende opmærksomhed i travle afdelinger. Dette kan føre til, at domæner, som fortsat anvendes aktivt – og i nogle tilfælde er kritiske for virksomhedens kommunikation, drift og brandbeskyttelse – uforvarende frigives og potentielt overtages af uvedkommende.

2. Sikkerhedsrisiko ved teknisk afhængighed

Mange virksomheder anvender domæner i tekniske infrastrukturer, hvor fx IoT-enheder, sensorer eller systemintegrationer er hardcodet til at kontakte specifikke URL'er (fx *update.vendor123-support.dk*). I disse tilfælde opfattes domænet som teknisk aktivt, men der

er ofte ikke etableret interne procedurer til håndtering af en særskilt årlig bekræftelse af kontaktoplysninger.

Hvis et sådant domæne slettes og efterfølgende registreres af en ondsindet aktør, kan der opstå alvorlige sikkerhedsbrud – uden at virksomhedens eget netværk kompromitteres. Det åbner mulighed for fx:

- **Man-in-the-middle-angreb** på datapakker,
- **Supply chain hijacking** via falske firmwareopdateringer,
- **Fuld overtagelse af enheder**, der ukritisk kommunikerer med domænet.

Det gør det klart, at domænesletning ikke blot er et administrativt eller forretningsmæssigt anliggende, men et potentielt angrebspunkt med reelle cyberrisici.

DI anbefaler derfor:

- At der suppleres med en differentieret tilgang til krav om bekræftelse, der tager højde for domænets anvendelseskontekst (fx teknisk/infrastrukturel brug).
- At bekendtgørelsen stiller krav om karenperiode før et domæne kan frigives efter sletning – navnlig for domæner, som har haft teknisk aktivitet.
- At der indføres varslinger i flere trin, herunder med krav om eksplicit advarsel til registranten før suspension eller sletning.
- At det tydeliggøres, at et domæne ikke må kunne overgå til en ny registrant i en periode (f.eks. 90 dage), medmindre tidligere registrant aktivt frasiger sig domænet.

Behov for proportionalitet og varsling

Kravet om aktiv respons bør afløses af en trinvist eskalerende varsling ved manglende bekræftelse – kombineret med karenperiode, før domænet kan frigives. Det sikrer både datasikkerhed, forretningskontinuitet og retssikkerhed.

Verifikationsform og metodefrihed (§ 3)

Det bør præciseres, at der alene kræves én kontaktmetode – i overensstemmelse med både direktivets betragtninger og ICANN-standarder. Der bør også gives metodefrihed i, hvordan en operationel verifikation konkret gennemføres, frem for at stille implicitte krav om aktiv respons, der er uhjemlet og sårbart overfor fejlfortolkning og phishingfrygt.

Hasteanmodninger (§ 6)

Det fremgår af høringsbrevet, at 24-timersfristen for hasteanmodninger går videre end det, der kræves i henhold til NIS2-direktivet. Det skaber praktiske og retlige problemer, især for små

registratorer og virksomheder uden døgnbemanding. En frist på fx 72 timer – evt. med mulighed for forkortelse i særligt alvorlige tilfælde – vil bedre balancere sikkerhedsbehov og administrativ realisme.

DI opfordrer til, at bekendtgørelsen justeres i retning af en mere risikobaseret, proportional og driftsnær tilgang, der sikrer cybersikkerhed uden at skabe uforholdsmæssige byrder eller utilsigtede sårbarheder for danske virksomheder.

Jeppe Engell
Chefkonsulent

29. april 2025

DIFO's bemærkninger til udkast til bekendtgørelse om validering, verifikation og udlevering af domænenavnsregistreringsdata

Digitaliseringsstyrelsen har den 26. marts 2025 sendt udkast til bekendtgørelse om validering, verifikation og udlevering af domænenavnsregistreringsdata i høring.

DIFO takker for denne mulighed for at afgive bemærkninger til Digitaliseringsstyrelsens udkast til bekendtgørelse. DIFO støtter, at der inden for de rammer, der er fastlagt i forbindelse med NIS2-lovforslaget udstedes en bekendtgørelse, der uddyber og præciserer NIS2-lovforslagets § 11.

DIFO kan dog konstatere, at bekendtgørelsesudkastet på flere punkter går videre end NIS2-lovforslagets tilsigtede minimumsimplementering af det bagvedliggende NIS2-direktiv. Dette har ifølge DIFO i hovedtræk følgende negative konsekvenser:

- Danske virksomheder og borgere påføres som registranter af et .dk-domænenavn uforholdsmæssige verifikationskrav med den risiko, at .dk-domænenavne fravælges til fordel for mindre sikre domænenavne og derved med risiko for en generelt dårligere cybersikkerhed i strid med intentionen i NIS2-direktivet og NIS2-loven.
- Danske virksomheder, herunder administratorer og forhandlere, pålægges flere administrative byrder i relation til procedurer for såvel verifikation som udlevering af domænenavnsregistreringsdata end andre tilsvarende europæiske virksomheder,

hvorved der skabes ulige konkurrencevilkår i forhold til administratorer og forhandlere i resten af Europa.

Samtidig savner DIFO, at det aktuelle bekendtgørelsesudkast skaber større klarhed om, hvem der må anses som "legitime adgangssøgende".

DIFO uddyber sine bemærkninger nærmere nedenfor.

Bekendtgørelsesudkastet går videre end NIS2-direktivet

Bekendtgørelsesudkastet udmønter i det store hele NIS2-samarbejdsgruppens anbefalinger til NIS2-direktivets artikel 28. NIS2-samarbejdsgruppen anbefaler bl.a., at både e-mail og telefonnummer verificeres, og at dette sker ved registreringen af nye domænenavne og ved fornyelse af eksisterende domænenavne. NIS2-arbejdsgruppen anbefaler også, at der ved hasteanmodninger fra legitime adgangssøgende gives adgang til domænenavnsregistreringsdata inden for 24 timer, ligesom der åbnes op for, at øvrige adgangssøgende kan anmode om data. Idet NIS2-samarbejdsgruppens anbefalinger i det store hele videreføres i bekendtgørelsesudkastet, kan DIFO konstatere, at bekendtgørelsesudkastet dermed går videre end det bagvedliggende NIS2-direktiv og NIS2-lovforslagets tilsigtede minimumsimplementering.

Udvidelsen sker ifølge DIFO på et tvivlsomt hjemmelsgrundlag, hvor flere af kravene i bekendtgørelsesudkastet ikke kan genfindes i hverken lovteksten i NIS2-direktivets artikel 28 eller NIS2-lovforslagets § 11. DIFO uddyber dette længere nede i relation til de enkelte bestemmelser.

Uforholdsmæssige verifikationskrav for danske borgere og virksomheder med risiko for dårligere cybersikkerhed

DIFO finder, at verifikationskravene i det aktuelle bekendtgørelsesudkast vil medføre, at danske virksomheder og borgere påføres betydelige ekstra byrder og omkostninger, idet de – for at opretholde brugsretten til et domænenavn – vil skulle gennemføre uforholdsmæssige mange verificeringer af deres e-mailadresse og telefonnummer med den risiko, at deres domænenavn suspenderes, hvis blot én verificering ikke gennemføres.

Det kan få store sikkerhedsmæssige og forretningsmæssige konsekvenser, særligt for virksomheder, hvis registranten overser eller glemmer at verificere sine oplysninger på ny, og domænenavnet derpå suspenderes eller slettes. Således vil virksomhedens hjemmeside og e-mailservice, tilknyttet det aktuelle domænenavn, som konsekvens heraf ikke længere fungere. Det samme vil gælde for andre kritiske tjenester, som måtte være tilknyttet domænenavnet, såsom fx vand-, fjernvarme- og elforsyning. Endelig vil der, hvis domænenavnet slettes, også være en risiko for, at kriminelle opsamler domænenavnet og bruger det til at oprette falske hjemmesider eller e-mailadresser, som kan forveksles med den tidligere registrants navn eller brand.

Bekendtgørelsesudkastets krav om gentagne verifikationer kan i sidste ende føre til, at .dk-domænenavne anses som mere risikofyldte og generelt fravælges til fordel for andre domænenavne, som ikke er lige så sikre. Dette vil i praksis føre til et resultat, der er i strid med lovens formål om øget cybersikkerhed.

Ulige konkurrencevilkår på det europæiske marked for domænenavne

DIFO finder, at det forhold, at bekendtgørelsesudkastet fraviger en minimumsimplementering af det bagvedliggende NIS2-direktiv både i forhold til verifikationer og udlevering af domænenavnsregistreringsdata, indebærer, at danske virksomheder, herunder administratorer og forhandlere, pålægges flere byrder end andre tilsvarende europæiske virksomheder. Dette harmonerer ifølge DIFO dårligt med, at en minimumsimplementering ifølge bemærkningerne til NIS2-lovudkastet netop skal sikre, *"at danske virksomheder ikke pålægges flere byrder end andre europæiske virksomheder"*.

DIFO/Punktum dk og danske forhandlere vil som følge heraf blive stillet dårligere i konkurrencen med andre administratorer og forhandlere i Europa, som ikke pålægges samme omfattende verifikationskrav og korte frister til udlevering af oplysninger. DIFO forventer således, at antallet af registrerede .dk-domænenavne vil falde mærkbart som følge af Digitaliseringsstyrelsens vidtgående verificeringskrav i bekendtgørelsesudkastet. Dels fordi registranter vil søge over på andre domænenavnsendelser, og dels fordi udenlandske forhandlere vil fravælge at sælge .dk-domænenavne. DIFO skal i den forbindelse bemærke, at den danske zone i dag er blandt

de sikreste domæneområder i verden.¹ De omfattende krav, der ellers har til hensigt at øge cybersikkerheden, vil således virke kontraproduktive.

Mens de omfattende krav til verificeringer og korte frister for udlevering af oplysninger vil gøre det vanskeligere for mindre danske forhandlere at operere på det danske marked for domænenavne, frygter DIFO, at større forhandlere vil forlade det danske marked, som følge af de væsentlige ekstra byrder og omkostninger.

DIFO finder, at det er afgørende, at NIS2-direktivets artikel 28 implementeres ensartet i EU's medlemslande for at skabe lige konkurrencevilkår og modvirke såkaldt forumshopping.

DIFO vil i det nedenstående nærmere redegøre for, hvor bekendtgørelsesudkastet ifølge DIFO konkret går uforholdsmæssigt og unødvendigt langt i forhold til de rammer, der er fastlagt i NIS2-lovgivningen. DIFO vil i samme ombæring tillade sig at komme med nogle konkrete løsningsforslag, som DIFO mener i højere grad balancerer, hvad der er nødvendige og proportionelle krav i forhold til de bagvedliggende hensyn i NIS2-lovgivningen.

§ 3 Validerings- og verifikationsprocedurer for e-mailadresse og telefonnummer

Bekendtgørelsesudkastet er meget detaljeret i sin beskrivelse af, hvordan administratorer og forhandlere skal sikre, at domænenavnsregistreringsdata er nøjagtige og fuldstændige.

DIFO verificerer gennem sit driftsselskab, Punktum dk, allerede i dag på forskellig vis registranternes navn, adresse og telefonnummer og har således etableret forskellige praksisser for netop at sikre, at de pågældende oplysninger er korrekte og opdaterede. Det samme har forhandlere, som også sælger andre domænenavne end .dk-domænenavne.

¹ Statisk fra DNS Research Federation viser, at misbrug på danske domænenavne er under 0,05 pct. Statistik fra CENTR viser, at .dk er det landedomænenavn i EU med den højeste udbredelse af DNSSEC (67,1 pct), som sikrer, at internetbrugere ikke ledes over på falske hjemmesider ved at manipulere DNS-forespørgsler.

Bekendtgørelsesudkastets detaljerede beskrivelse risikerer ifølge DIFO at hindre allerede velfungerende verifikationsmetoder samt besværliggøre, eller måske endda umuliggøre, fremtidige bedre verifikationsmetoder.

DIFO skal derfor henstille til, at der gives metodefrihed på samme måde, som der i dag gives i domæneloven. Dette vil sikre, at bekendtgørelsen ikke i fremtiden hindrer anvendelsen af de bedst egnede verifikationsmetoder og -procedurer.

DIFO anerkender, at der kan være behov for at gå videre end ICANN's regler i forhold til verifikation af registranter. DIFO finder imidlertid, at dette allerede er sket gennem verifikation af registranters identitet.

Tidspunkt for verifikation af registrantens oplysninger – § 3, stk. 1

Bekendtgørelsesudkastet stiller i sin ordlyd kun krav om verifikation af e-mailadresse og telefonnummer ved enten registreringen eller ved hver fornyelse.

Verifikation af e-mailadresse og telefonnummer – § 3, stk. 1

Det fremgår af NIS2-direktivets præambelbetragtning 111, som er gengivet i bemærkningerne til NIS2-lovforslagets § 11, stk. 3, at fastlagte og indførte verifikationsprocedurer skal være forholdsmæssige og, at navnlig mindst én kontaktmåde for registranten bør verificeres. Herved skal forstås, at de krav, der stilles, ikke må gå længere end nødvendigt, og at én kontaktmåde vurderes at være tilstrækkelig til at opfylde lovens formål om at kunne identificere og kontakte registranter.

DIFO bemærker, at bekendtgørelsesudkastet stiller krav om validering og verifikation af både kontakt-e-mailadresse og telefonnummer. Dette går imod såvel bemærkningerne til NIS2-lovforslagets § 11, stk. 3, NIS2-direktivets betragtning 111 som ICANN's standarder. Bekendtgørelsesudkastet går således videre end den minimumsimplementering, som lovforslaget angiver, skal foretages. Der henvises herom i øvrigt til DIFO's bemærkninger til bekendtgørelsesudkastets § 6.

DIFO bemærker, at der for .dk-domænenavne i henhold til domæneloven tillige er et krav om at sikre retvisende oplysninger om postadresse. Opretholdes kravet i bekendtgørelsesudkastet om validering og verifikation af både e-mailadresse og telefonnummer, vil der for .dk-

domænenavne være krav om omfattende verifikationer af tre forskellige kontaktmåder. Dette går ifølge DIFO langt ud over, hvad der må anses for nødvendigt til at opfylde formålet med NIS2-lovforslagets § 11 om at kunne komme i kontakt med registranten.

Foreslået alternativ til § 3, stk. 1

DIFO finder på baggrund af det ovenstående om såvel tidspunkt som kontaktmåde, at teksten i § 3, stk. 1, bør ændres til:

§ 3 Ved registrering af et domænenavn eller ved første fornyelse af et eksisterende domænenavn skal topdomænenavneadministratorer og enheder, der leverer domænenavnsregistreringstjenester, sikre, at registrantens kontakt e-mailadresse eller telefonnummer er syntaktisk valideret og operationelt verificeret i medfør af stk. 4, jf. dog stk. 6.

Gentagne verifikationer – § 3, stk. 5

DIFO forstår denne bestemmelse som en lempelse til kravet i § 3, stk. 1.

Som bestemmelsen er formuleret, indebærer den, at verifikation ved fornyelse kan undlades, hvis registranten har anvendt eID og *hvert eneste* år siden registreringen af domænenavnet aktivt har bekræftet både sin e-mailadresse og sit telefonnummer. Som bestemmelsen er formuleret, medfører den ifølge DIFO derfor ingen reel lempelse for de registranter, der har anvendt eID. DIFO bemærker hertil, at langt de fleste registranter registrerer et domænenavn for ét år ad gangen.

Indføres der krav om gentagne verifikationer, vil dette i konkrete tal indebære at ca. 710.000 registranter vil skulle gennemføre en verifikation hvert år med risiko for at miste brugsretten til deres domænenavne. Hertil kommer et ukendt antal registranter af andre domænenavns-ender.

Kravet om gentagne verifikationer kan med høj sandsynlighed føre til, at flere tusinde registranter, herunder virksomheder, vil få suspenderet eller slettet deres domænenavne, selv om deres oplysninger er korrekte, alene fordi registranten overser eller glemmer at gennemføre verifikationen. Denne risiko for, at en verifikation ikke gennemføres, skal tillige ses i lyset af den sam-

fundsmæssige skepsis, der efterhånden er opstået, mod at klikke på links i e-mails eller sms'er af frygt for at blive udsat for phishing mm.

Når registranten både har gennemført en MitID-kontrol, og oplysningerne er matchet og låst til CPR/CVR-registreret, hvorved navn og adresse opdateres automatisk, synes det ifølge DIFO overflødigt, at registranten samtidig selv skal gøre noget aktivt hvert år for ikke at miste brugsretten til sit domænenavn, med de risici dette indebærer, jf. ovenfor.

Samtidig bemærkes, at kravet om gentagne verifikationer primært synes at ramme registranter, der har et legitimt formål med at bruge et domænenavn, idet misbrug på domænenavne som alt overvejende hovedregel sker inden for den første registreringsperiode, og typisk kort tid efter domænenavnet er blevet registreret.

Forslået alternativ til § 3, stk. 5

DIFO finder, at § 3, stk. 5, bør udgå som led i ovenstående ændringsforslag til § 3, stk. 1. DIFO finder, at der alene bør 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 disse oplysninger ikke er korrekte. Dette balancerer i højere grad de nødvendige tiltag med henblik på at sikre, at kontaktoplysninger er korrekte. Dette kunne ifølge DIFO evt. indføres i oplistningen i § 3, stk. 3.

Hvis stk. 1 ikke ændres som foreslået, foreslår DIFO at give bestemmelsen i stk. 5 et reelt indhold og virkningsområde og således lempe kravet til verifikationer af e-mailadresse og telefonnummer, hvor der er anvendt eID. DIFO finder i dette tilfælde, at § 3, stk. 5, bør ændres til:

Stk. 5 Hvis elektronisk identifikation anvendes til at verificere en registrants navn efter stk. 1, og registranten mindst én gang årligt anmodes om at bekræfte sin kontakt e-mailadresse og telefonnummer, kan den syntaktiske validering og operationelle verifikation af registrantens kontakt e-mailadresse og telefonnummer efter stk. 1 undlades ved fornyelsen af et domænenavn.

Én verifikation ved flere domænenavne under samme topdomænenavn – § 3, stk. 6

DIFO mener, at en validering og verifikation af en registrants identitet og kontaktoplysninger skal kunne genbruges, hvis registranten har registreret flere domænenavne med samme kontakt-

oplysninger på tværs af forskellige topdomænenavne. Det giver ifølge DIFO meget lidt mening, at en registrant skal verificere sit navn og sine kontaktoplysninger flere gange, bare fordi vedkommende registrerer både et fx .com og .nu-domænenavn frem for to .com-domænenavne. Bestemmelsen i sin nuværende ordlyd forhindrer også, at ccTLD'er på tværs af EU, fx den svenske Internetstiftelse og DIFO/Punktum dk, kan genbruge hinandens verifikationer, fx ved brug af den kommende EU-wallet.

Forslået alternativ til § 3, stk. 6

DIFO foreslår, at den begrænsning, der ligger i bestemmelsen om, at verifikationer kun kan bruges, hvis de knytter sig til samme topdomænenavn, fjernes.

§ 5 Manglende validering eller verifikation af domænenavsregistreringsdata

Suspension eller sletning ved manglende validering eller verifikation ved fornyelse – § 5, stk. 2

DIFO finder, 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, hvis registranten samtidig har verificeret både sin identitet og e-mailadresse, og for .dk-domænenavne tillige sin postadresse.

Suspension og sletning af domænenavne kan indebære uoprettelige konsekvenser for borgere og virksomheder, jf. ovenfor, og bør derfor ikke anvendes i større omfang end absolut nødvendigt.

DIFO skal tillige bemærke, at hvis domænenavnet, der suspenderes, bruges til en e-mail, vil registranten ikke efterfølgende i suspensionsperioden kunne validere sin e-mailadresse, da denne ikke længere virker.

DIFO finder således, at formålet om, at man skal kunne komme i kontakt med registranten, må anses som tilstrækkeligt opnået, hvis én kontaktmåde er verificeret. Særligt, når dette afvejes i

forhold til de omfattende konsekvenser, det kan have for en registrant at få suspenderet sit domænenavn.

Foreslået alternativ til § 5, stk. 2

På baggrund af det ovenstående foreslår DIFO derfor, at der ikke sker suspension på grund af manglende validering og verificering af kontakt e-mailadresse eller telefonnummer, hvis én kontaktmåde allerede er verificeret. Dette kan fx indføres med et nyt stk. 3, med følgende ordlyd:

Stk. 3 Suspension eller sletning efter stk. 2 på grund af manglende syntaktisk validering og operationel verificering af kontakt e-mailadresse eller telefonnummer skal dog ikke finde sted, hvis mindst én kontaktmåde for registranten allerede er syntaktisk valideret og operationelt verificeret.

§ 6 Anmodninger om adgang til domænenavnsregistreringsdata

Udlevering af oplysninger til legitime adgangssøgende – § 6, stk. 1

Det fremgår af bekendtgørelsesudkastets § 6, stk. 1, at administratorer og forhandlere på baggrund af en *lovlig og behørig begrundet anmodning* fra en *legitim adgangssøger* skal give adgang til specifikke domænenavnsregistreringsdata uden unødigt ophold og under alle omstændigheder inden for 72 timer samt i tilfælde af *hasteanmodninger* inden for 24 timer.

Hvis det skal være reelt muligt at leve op til denne bestemmelse, er det nødvendigt, at bestemmelsen er mere klar og operationel i forhold til, hvem der kan anses som legitime adgangssøgende, herunder har det lovlige grundlag for en anmodning om udlevering af oplysninger. Uden klare og operationelle retningslinjer må det forventes, at der vil blive fastlagt en meget forsigtig og restriktiv praksis for udlevering af oplysninger.

Om 24-timersfristen for hasteanmodninger

Digitaliseringsstyrelsen har i forbindelse med høringen over nærværende bekendtgørelsesudkast selv tilkendegivet, at bekendtgørelsen med indførelsen af en 24-timersfrist for behandling af hasteanmodninger går videre end en minimumsimplementering af det bagvedliggende

direktiv. Digitaliseringsstyrelsen har som grundlag herfor henvist til at kunne gribe ind i særligt kritiske situationer.

DIFO finder ikke blot, at ovenstående udgør en overimplementering i forhold til det bagvedliggende NIS2-direktiv, men også at det er funderet på et lovgivningsmæssigt tvivlsomt grundlag.

Således bemærkes, at der *ikke* fremgår nogen 24-timersfrist i NIS2-lovforslagets § 11, stk. 5, som ifølge bemærkningerne til loven udgør en indholdsmæssig implementering af NIS2-direktivets artikel 28, stk. 5, og skal forstås og anvendes i overensstemmelse med direktivets forudsætning.

DIFO finder det betænkeligt, at Ministeriet for Samfundssikkerhed og Beredskab efter høringen over udkastet til NIS 2-lovforslaget i forbindelse med den senere fremsættelse af lovforslaget den 6. februar 2025 for Folketinget via lovbemærkningerne til lovforslagets § 11, stk. 8, har indført, at de administrative forskrifter digitaliseringsministeren kan udstede, kan ske på baggrund af retningslinjer udarbejdet af Europa-Kommissionen, ENISA eller Samarbejdsgruppen nedsat iht. NIS2-direktivet. DIFO finder det herpå betænkeligt, at der tillige i lovbemærkningerne er indført, at denne bemyndigelsesbestemmelse bl.a. kan anvendes til at fastsætte bestemmelser om tidsrammerne for udlevering af oplysninger ved hasteanmodninger, og at der derved via lovbemærkningerne er indført en mulighed for at pålægge en forpligtelse, der går videre end bestemmelsen i det bagvedliggende NIS2-direktiv.

DIFO konstaterer i den forbindelse, at Ministeriet for Samfundssikkerhed og Beredskab både i betænkningen afgivet af Forsvars-, Samfundssikkerheds- og Beredskabsudvalget den 10. april 2025 og af den kommenterede oversigt over høringssvar vedrørende forslag til NIS2-loven har undladt at oplyse, at man efter den offentlige høring over forslaget til NIS2-loven har foretaget væsentlige ændringer i lovforslaget, der muliggør overimplementering af NIS2-direktivet. Ministeriet oplyser derimod i den kommenterede oversigt, at der ud over enkelte ændringer nævnt i oversigten kun er foretaget ændringer af *sproglig, redaktionel og lovteknisk karakter*. Dette er ikke korrekt, og overimplementeringen rammer ikke kun administratorer og forhandlere, men alle danske virksomheder og borgere, der har registreret et domænenavn.

Til trods for ovenstående bemærkninger forstår og anerkender DIFO det saglige hensyn og behov for via proportionale forpligtelser i NIS2-lovgivningen at øge den generelle cybersikkerhed. DIFO bemærker dog, at Digitaliseringsstyrelsen med sin begrundelse om hensynet til

tilfælde af misbrug af børn – om end DIFO er enig i, at dette udgør et vigtigt hensyn – går videre end formålet i NIS2-lovgivningen om øget cybersikkerhed.

DIFO skal i den forbindelse gøre opmærksom på, at registranten af et domænenavn ikke nødvendigvis altid er den samme som den, der står bag og ejer den tilhørende hjemmeside, hvorfra en kriminel handling eller cybertrussel hidrører. Der er således med forpligtelsen ingen garanti for tilvejebringelsen af den relevante kontaktinformation om gerningspersonen, ligesom det ikke direkte stopper en konstateret trussel.

Endelig bemærker DIFO, at forpligtelsen til at udlevere domænenavsregistreringsdata inden for de givne frister såvel for DIFO/Punktum dk som for både store og små forhandlere, indebærer nødvendigheden af en vagtordning. Dette kan for nogle forhandlere være en meget byrdefuld konsekvens af forpligtelsen, der som beskrevet ovenfor ikke nødvendigvis medfører udlevering af kontaktoplysninger, der fører frem til den aktuelle gerningsperson.

Såfremt Digitaliseringsstyrelsen finder, at det er nødvendigt og proportionalt at fastholde indførelsen af en 24-timersfrist for hasteanmodninger, er det DIFO's opfattelse, at dette i endnu højere grad nødvendiggør behovet for yderligere klarhed om, hvem der må anses som *legitime adgangssøgende*, herunder at disse har det lovlige grundlag for en anmodning om udlevering af oplysninger.

Om legitime adgangssøgende

DIFO bemærker, at der i bekendtgørelsesudkastet ikke – som forventet – er nogen nærmere præcisering i forhold til, hvad der allerede fremgår af NIS2-lovforslaget, jf. lovbemærkningerne til § 11, stk. 5, om, hvem der må anses som *legitime adgangssøgende*, herunder om dette også omfatter privatpersoner eller virksomheder samt juridiske og fysiske personer/myndigheder, uden for Danmark. Således fremgår alene af § 2, nr. 7 i bekendtgørelsesudkastet en forholdsvis bred definition af legitime adgangssøgende.

Det skaber den paradoksale situation, at lovbemærkningerne til § 11, stk. 5, i NIS2-lovforlaget er mere præcise end bekendtgørelsesudkastet i sin præcisering af legitime adgangssøgende, hvorfor NIS2-lovforslagets bemærkninger pt er den eneste kilde til fortolkningsgrundlag i forhold til den nærmere afklaring af, hvem der må anses som legitime adgangssøgende.

Hvis legitime adgangssøgende også omfatter juridiske og fysiske personer uden for Danmark, savner DIFO i relation til det forelagte bekendtgørelsesudkast afklaring og retningslinjer for, hvordan DIFO/Punktum dk og forhandlere skal kunne vurdere, om en ansøger, der udgiver sig for at være en myndighed, reelt er, hvad den udgiver sig for at være, og om den har et lovligt grundlag. Samme gør sig i endnu højere grad gældende for privatpersoner og virksomheder i udlandet, som DIFO/Punktum dk ikke kender sikre metoder til at afgøre, hvorvidt sådanne er "svindlere" eller reelle i den forstand, at de har den påståede saglige grund til at få udleveret de ønskede oplysninger.

Forslået alternativ til § 6, stk. 1

Med henblik på at gøre det reelt muligt for DIFO/Punktum dk og forhandlere at leve op til kravene i det forelagte bekendtgørelsesudkasts § 6, stk. 1, om udlevering af domænenavns-registreringsdata, har DIFO derfor følgende konkrete ønsker:

1. At der fra myndighedernes side udarbejdes en udtømmende liste over, hvem der anses som de nationale legitime adgangssøgende.
2. At det for så vidt angår udenlandske adgangssøgende præciseres, at disse alene kan anses som legitime adgangssøgende, hvis en dansk domstol, administrativ myndighed eller ENISA (på EU-plan) forinden har fastslået, at de er at anse som legitime adgangssøgende.
3. At det præciseres, at DIFO/Punktum dk og forhandlere kan lægge disse legitime adgangssøgendes begrundelse om nødvendighed og lovhjemmel til grund, uden at skulle foretage en selvstændig prøvelse heraf.

Udlevering af oplysninger til øvrige adgangssøgende – § 6, stk. 3

Det fremgår af bekendtgørelsesudkastets § 6, stk. 3, at administratorer og forhandlere på baggrund af en behørig begrundet anmodning fra *øvrige adgangssøgende* om specifikke ikke-offentliggjorte domænenavnsregistreringsdata inden for 72 timer skal oplyse, om denne adgang gives.

DIFO finder det betænkeligt, hvorvidt denne bestemmelse – som i praksis også vil omfatte oplysninger om borgere, som har navne- og adressebeskyttelse – har den fornødne lovgivnings-

mæssige hjemmel i NIS2-lovforslaget. Det skyldes, at begrebet "øvrige adgangssøgende" ikke kan genfindes i lovteksten til § 11 i NIS2-lovforslaget, men at der er tale om et begreb, som alene er kommet ind via bemærkningerne til NIS 2-lovforslagets § 11, stk. 8.

I tråd med DIFO's ovenstående bemærkninger i relation til indførelsen af en 24-timersfrist for hasteanmodninger, finder DIFO det tilsvarende betænkeligt, at indførelsen af en bestemmelse, hvorefter alle andre end legitime adgangssøgende kan søge om udlevering af ikke-offentliggjorte domænenavnsregistreringsdata, er sket via NIS2-lovforslagets bemærkninger og ikke direkte via en hjemmel i NIS2-lovforslaget.

DIFO skal endelig bemærke, at det synes uvist, hvad formålet med bestemmelsen i § 6, stk. 3, om udlevering af oplysninger til øvrige adgangssøgende er, herunder hvordan dette bidrager til formålet i NIS2-lovgivningen om øget cybersikkerhed.

Foreslået alternativt til § 6, stk. 3

Det er på baggrund af ovenstående bemærkninger DIFO's opfattelse, at bestemmelsen om udlevering af oplysninger til øvrige adgangssøgende i bekendtgørelsesudkastets § 6, stk. 3, bør udgå.

Ikrafttrædelse – § 9

DIFO skal ud over ovenstående anmode 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.

Til Digitaliseringsstyrelsen

Vi værdsætter muligheden for at afgive høringssvar til Digitaliseringsstyrelsens udkast til bekendtgørelse om validering, verifikation og udlevering af domænenavsregistreringsdata ("registreringsdata").

Nærværende høringssvar er underskrevet af mere end 60 danske og internationale organisationer og virksomheder på tværs af internetsamfundets aktører. Blandt underskriverne er enheder, der leverer domænenavsregistreringstjenester ("forhandlere"), topdomænenavneadministratorer ("administratorer") samt branche- og interesseorganisationer. Det er vores vurdering, at medunderskriverne tilsammen repræsenterer over 95 % af alle domæner i .dk-zonen.

Blandt underskriverne kan særligt fremhæves:

- *eco – Association of the Internet Industry*, Europas førende brancheorganisation med cirka 1.000 medlemmer, hvor *Names & Numbers Working Group* dækker over 70% af alle registrerede domæner globalt, samt
- *ICANN Registrar Stakeholder Group (RrSG)*, som repræsenterer domæneadministratorer globalt og er en central aktør i forvaltningen af internettets domænenavnesystem.

Vores største bekymring med den foreslåede tekst er at bekendtgørelsen går videre end en de krav der stilles i EU's NIS 2-direktiv samt alle nuværende foreslåede eller vedtagne lovgivninger og direktiver i andre EU-medlemsstater.

En implementering af bekendtgørelsen i sin nuværende form, truer med at stille danske virksomheder, der er aktive på det europæiske og globale marked for domænenavnstjenester, ringere end deres udenlandske konkurrenter. Det er netop denne situation, som den danske lovgiver søgte at undgå ved gennemførelsen af NIS 2-direktivet: "*Ved at anvende minimums-implementering sikres det, at danske virksomheder ikke pålægges flere byrder end andre europæiske virksomheder*".¹

De følgende afsnit forklarer, hvor og hvordan udkastet går videre end en minimumsimplicitering af direktivet, hvorfor dette skaber praktiske og økonomiske problemer, og hvordan mere afbalancerede alternativer kunne se ud.

¹ Lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau (NIS 2-loven) s. 21

1) Operationel verifikation af e-mailadresse OG telefonnummer (Kapitel 2, §3)

- A. Den foreslåede verifikation går videre end minimumskraverne i EU-direktivet, gældende branche-standarder og kravene i andre medlemsstater.

I NIS 2-direktivets præambelbetragtning 111 samt den danske NIS 2-lov² fremgår det at politikkerne og procedurerne nævnt i artikel 28 i NIS 2 "*så vidt muligt skal tage hensyn til de standarder, der er udviklet af multiinteressentstyringsstrukturerne på internationalt plan*" og "*bør afspejle industriens best practice*"

Præambelbetragtning 111 henviser klart til branchestandarden³ udviklet af ICANN, da der ikke findes andre multiinteressentstyringsstrukturer på internationalt plan. Denne standard gælder for alle gTLDer⁴ og kræver kun operationel verifikation af én kontaktmåde (enten e-mailadresse eller telefonnummer). De fleste forhandlere har valgt at implementere e-mailverifikation, da det er den eneste kontaktmåde, der er nødvendig for at administrere et domæne. Dette er helt i overensstemmelse med præambelbetragtning 111 samt den danske NIS 2-lov, som siger "*Topdomænenavneadministratorerne og de enheder, der leverer domænenavnsregistreringstjenester, bør navnlig verificere mindst én kontaktmåde for registranten.*"⁵

Bekendtgørelsen er baseret på anbefalinger fra NIS Cooperation Group, som foreskriver, at både telefonnummer og e-mailadresse skal verificeres. NIS Cooperation Group består udelukkende af repræsentanter for EU's NIS 2-myndigheder og er hverken international eller multiinteressent-styret. Der er intet, der tyder på, at NIS Cooperation Group har inddraget forhandlere, før gruppen vedtog sine anbefalinger. Anbefalingerne fra NIS Cooperation Group er indtil videre ikke blevet implementeret af nogen EU-medlemsstat. Danmark ville være det første - og muligvis eneste - land som implementerer disse anbefalinger.

- B. Implementering af verifikation af både e-mailadresse OG telefonnummer vil pålægge danske forhandlere en yderligere byrde sammenlignet med andre europæiske forhandlere og vil ikke have nogen mærkbare effekt for DNS' sikkerhed, stabilitet og modstandsdygtighed

Resultatet af den foreslåede bekendtgørelse 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.

² Lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau (NIS 2-loven) s. 71

³ ICANN RDDS Accuracy Program Specification (<https://www.icann.org/en/system/files/files/registrars-accreditation-agreement-21jan24-en.htm#rdds-accuracy>)

⁴ Domænenavne som ikke er forbundet med et land. De mest almindelige er .com, .org og .net. Alle gTLDer hører under ICANN's politikker. Ca. halvdelen af alle registrerede domæner i verden er gTLDer.

⁵ Lov om foranstaltninger til sikring af et højt cybersikkerhedsniveau (NIS 2-loven) s. 71

At implementere et system til verifikation af telefonnumre for hver registrering og for registranter over hele verden er ikke en triviell opgave. Kravet om operationel verifikation af telefonnumre vil øge kompleksiteten, skabe friktion i kunderejsen, og vil 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.

Selv hvis verifikation af telefonnumre var en effektiv metode i bekæmpelsen af cyberkriminalitet (hvilket er diskutabelt), vil potentielle svindlere - både danske og udenlandske – nemt kunne undgå verifikationen ved blot at bestille et TLD, der ikke kræver telefonverifikation, som .com, fra en ikke-dansk virksomhed.

Ikke-danske forhandlere kunne også vælge helt at stoppe med at tilbyde topdomænenavne ("TLDer") fra danske administratorer for at undgå kravet om operationel verifikation af telefonnummeret. Dette ville have en negativ indvirkning på de danske administratorer.

C. Foreslået alternativ: verifikation af mindst én kontaktmåde

Skulle bekendtgørelsens bestemmelser om e-mail- og telefonverifikation blive vedtaget, vil Danmark være det eneste land i verden (indtil videre), der pålægger sine forhandlere og administratorer kravet om at verificere både e-mailadresse og telefonnummer. Det vil medføre en konkurrencemæssig ulempe for danske virksomheder og skabe gnidninger for registranterne - uden at bidrage væsentligt til DNS' sikkerhed, stabilitet og modstandsdygtighed, som omtalt i artikel 28, stk. 1, i NIS 2-direktivet.

Vi foreslår derfor, at bekendtgørelsen bringes i overensstemmelse med den branchestandard, der er udviklet af ICANN⁶, og alene kræver operationel verifikation af mindst én kontaktmåde.

2) Unødvendig begrænsning i muligheden for genbrug af verifikation på tværs af TLDer (Kapitel 2, §3 Stk. 6; Kapitel 3, §4, Stk.6)

A. Unødvendig genverificering af identiske data på tværs af TLDer

Bekendtgørelsen fastsætter, at *"hvis en registrant registrerer eller har registreret flere domænenavne under samme topdomænenavn, er det tilstrækkeligt [...] at verificere registrantens navn [...] for ét af registrantens domænenavne."*

Vi forstår ikke, hvorfor denne undtagelse er begrænset til domæner under samme TLD. Begrænsningen virker unødvendig og kunne uden problemer udvides til også at omfatte domæner under forskellige TLDer, så længe registranten og registreringsdata er identiske.

⁶ ICANN RDDS Accuracy Program Specification (<https://www.icann.org/en/system/files/files/registrar-accreditation-agreement-21jan24-en.htm#rdds-accuracy>)

Dette ville gøre det muligt for forhandlere kun at gennemføre verifikation én gang for den samme registrant, selv når registranten bestiller flere domæner under forskellige TLDer (f.eks. et .com- og et .se-domæne).

På den måde undgår man, at forhandlere og registranter skal verificere de samme data flere gange, muligvis endda i forbindelse med den samme ordre, uden at gå på kompromis med registreringsdataenes nøjagtighed.

B. Foreslået alternativ: verifikation på registrantniveau

Der er ingen saglig begrundelse i at kræve separat verifikation, når registranter bestiller forskellige TLDer. Det skaber unødvendige gentagelser for både forhandlere og registranter - især når flere domænenavne under forskellige TLDer bestilles samtidigt. Det bør ikke være nødvendigt at verificere den samme registrant mere end én gang, hvis de angivne oplysninger er identiske.

Vi foreslår derfor at ændre Kapitel 2, §3 Stk. 6 og Kapitel 3, §4, Stk. 6 med henblik på at muliggøre genbrug af verifikation på tværs af TLDer, hvor de registreringsdata, som registranten har oplyst, er identiske.

En revision af reglen, der tillader genbrug af verifikation på tværs af TLDer, vil være i overensstemmelse med proportionalitetsprincip i NIS 2-direktivets og med den danske lovgivers hensigt om at undgå unødvendige byrder for danske virksomheder.

3) Krav om at verificere registreringsdata før aktivering af domænet (Kapitel 4, §5)

A. For mange TLDer er det ikke teknisk muligt for registratorer at forhindre domæneaktivering, før verifikationen er gennemført.

Bekendtgørelsen kræver, at domænenavne ikke må aktiveres, før registreringsdata er verificeret. Dette er dog ikke teknisk muligt for mange landekodetopdomæner (ccTLDer).⁷

Mens gTLD-administratorer giver forhandlere mulighed for at anvende en *clientHold*-status, som deaktiverer DNS for pågældende domæne, tilbyder de fleste ccTLD-administratorer ikke en lignende mekanisme. I mange tilfælde bliver domæner automatisk aktive ved registrering, og forhandlerne har ingen mulighed for at forsinke aktiveringen.

Forhandlere, der også driver DNS-infrastruktur, kan muligvis henvise domænerne til navneservere, der ikke svarer for et givent domæne, mens de afventer verifikation. Denne løsning kan dog være i strid med nogle ccTLD-administratorers krav til forhandlerne, om funktionelle navneservere på registrerings-

⁷ Domænenavne som er forbundet med et land. f.eks. .dk, .se, .fi, .no, etc.

tidspunktet (som for .it domæner). Det betragtes også som bad practice, da sådan et set up har en negativ effekt på sikkerheden, stabiliteten og modstandsdygtigheden af DNS⁸

Forhandlere, som ikke er ansvarlige for DNS, har ingen tekniske muligheder for at forsinke aktiveringen af et domænenavn hvor en sådan mekanisme ikke tilbydes af TLD'ets administrator. Deres eneste mulighed vil være at udskyde registreringen helt, indtil verifikationen er gennemført, hvilket øger risikoen for, at domænet i mellemtiden er blevet registreret til anden side.

Vi foreslår, at bekendtgørelsen tillader, at verifikationen gennemføres efter registreringen, i stedet for at kræve, at den gennemføres, før et domæne kan aktiveres. 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. Det ville også afspejle den fleksibilitet, der tilbydes i præambelbetragtning 111 i NIS 2-direktivet, som udtrykkeligt tillader både ex ante og ex post verifikation.

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.

Derfor fastholder vi, at en enkel model, der tillader verifikation efter registrering for alle TLDer, er den mest afbalancerede og proportionelle løsning.

B. Foreslået alternativ: ex post verifikation

Kravet om, at verifikation skal gennemføres før aktivering, selvom bredt accepterede branchestandarder og EU-vejledning⁹ tillader verifikation efter registrering, går videre end det minimum, der kræves i NIS 2-direktivet. Det indfører uforholdsmæssigt store implementeringsbyrder for forhandlere og skabe konkurrenceforvridning i forhold til forhandlere i andre EU-medlemsstater. Dette vil have en negativ indvirkning på DNS' sikkerhed, stabilitet og modstandsdygtighed og medføre en risiko for, at domænenavne registreres andre steder i tiden mellem bestilling og verifikation.

Vi anbefaler derfor, at Kapitel 4, §5 i Bekendtgørelsen ændres, så domæner kan blive aktive ved registrering, og at verifikation kan finde sted inden for en bestemt tidsramme (f.eks. 15 dage). Suspension bør kun være påkrævet, hvis verifikationen ikke er afsluttet inden for denne periode

⁸ <https://www.ioriver.io/terms/lame-delegations>

<https://blog.apnic.net/2021/03/16/the-prevalence-persistence-perils-of-lame-nameservers/>

⁹ Se NIS 2-direktivets præambelbetragtning 111 og ICANN's 2013 RDDS Accuracy Program Specification nævnt ovenfor

4) Verifikation ved fornyelse (Kapitel 2, §3, stk. 1)

A. Fornyelsesbaseret verifikation går videre end gældende branchepraksis, medfører en uforholdsmæssig stor byrde og risikerer at føre til suspension af legitime domæner

Det nuværende udkast til bekendtgørelsen kræver, at validering og verifikation udføres ved registrering, ejerskifte og i forbindelse med domænefornyelse, selv når registreringsdata forbliver uændrede.

At kræve verifikation, blot fordi et domæne fornyes, går ud over både den minimumsstandard, der er fastsat i NIS 2-direktivet, og den praksis, der er defineret i ICANN RDDS Accuracy Program Specification. Dette vil stille forhandlere og administratorer ringere end deres europæiske modparter.

At bruge fornyelseshændelsen som udløser for verifikation er ikke en pålidelig måde at sikre, at registreringsdata forbliver opdaterede. Fornyelse er blot en teknisk faktureringsbegivenhed og afspejler ikke nødvendigvis nogen ændring i registranten eller dennes registreringsdata. Selv hvis kravet blev ændret til et fast interval, såsom årlig verifikation, ville det stadig medføre yderligere forpligtelser, som ikke udtrykkeligt kræves i henhold til NIS 2-direktivet, og det ville derfor være i strid med den danske lovgivers hensigt om at undgå unødige byrder for danske virksomheder sammenlignet med virksomheder i andre medlemsstater

Indførelse af anmodninger om genverificering ved fornyelse eller ved faste intervaller, uden at registranten har foretaget en handling, vil føre til mange suspenderinger af legitime domæner. Fornyelser sker normalt uden behov for handling fra registranten. Mange registranter vil ikke nå at reagere på kommunikationen i tide - eller kan forveksle den med et phishing-forsøg.

Det ville give langt mere mening at knytte verifikation til begivenheder, der kræver aktiv handling fra registranten, da registranten i disse tilfælde vil forvente at skulle reagere.

Når domænenavne suspenderes, deaktiveres alle tjenester der er forbundet med domænenavnet f.eks. hjemmesider, onlineportaler, platforme, e-mailtjenester, servere mv. Dette kan få alvorlige konsekvenser, hvis de berørte domænenavne anvendes af enheder der leverer væsentlig infrastruktur.

B. Foreslået alternativ: Begræns genverifikation til relevante ændringer eller begrundet tvivl om nøjagtighed

Vi foreslår, at kapitel 2 og 3 ændres, så kravet om at udføre validering og verifikation i forbindelse med domænefornyelse fjernes. I stedet bør bestemmelsen kun kræve verifikation ved registrering, ved ændring af relevante datafelter, eller når der er en begrundet årsag til at betvivle nøjagtigheden af de registrerede oplysninger.

Dette vil bringe den danske implementering i overensstemmelse med den internationale branchestandard¹⁰ og sikre proportionalitet i overensstemmelse med principperne i NIS 2-direktivet.

5) Krav om at give oplysninger til legitime adgangssøgende (kapitel 5 og 6)

A. Bekendtgørelsen afbalancerer ikke grundlæggende interesser og er i modstrid med den kommende e-evidensforordning

Vurderingen af "legitimiteten" af en myndigheds anmodning om at udlevere identifikationsoplysninger er kompliceret og omfatter en afvejning af borgerens grundlæggende ret til privatlivets fred og databeskyttelse med behovet for effektiv retsforfølgelse af strafbare handlinger. Afvejningen af disse interesser er afgørende for, at EU kan nå sit mål om at opretholde og udvikle et område med frihed, sikkerhed og retfærdighed.

EU-lovgiveren har anerkendt vigtigheden af at afbalancere de forskellige grundlæggende rettigheder og interesser, der er på spil, ved at vedtage e-evidensforordningen¹¹, som vil finde anvendelse fra den 18. August 2026. E-evidensforordningen vil gælde *"for internetdomænenavne og IP-nummereringstjenester såsom IP-adressetildeling, domænenavneregister, domænenavneregistrator og domænenavnerelaterede privatlivs- og proxytjenester"*. Denne forordnings anvendelsesområde overlapper klart med NIS 2, når det drejer sig om anmodninger om oplysninger. I modsætning til et direktiv er en forordning direkte bindende for alle medlemsstater, og medlemsstaterne har ikke lov til at indføre strengere regler.

E-evidensforordningen indeholder mange proceduremæssige og væsentlige krav for at sikre nødvendigheden og proportionaliteten af anmodninger om oplysninger. Den indeholder meget specifikke bestemmelser om, hvilke myndigheder der kan anmode om oplysninger (kun myndigheder, der retsforfølger straffelovsovertrædelser), hvilke oplysninger, under hvilke betingelser og inden for hvilken tidsramme (8 dage eller 96 timer i hastetilfælde).

E-evidensforordningen indeholder også bestemmelser, der giver tjenesteudbyderen ret til at gøre indsigelse mod en anmodning om oplysninger, og som sikrer, at den person, hvis registreringsdata der anmodes om, bliver informeret.

Bekendtgørelsen indeholder derimod slet ingen bestemmelser, der sikrer en afbalancering af de grundlæggende rettigheder. I stedet giver bekendtgørelsen et absolut skøn til en tilsynsmyndighed til at bestemme legitimiteten af en anmodning og den bøde, der skal betales for at nægte at efterkomme den - tilsyneladende uden nogen mulighed for appel. Den fastsætter ikke engang nogen standarder, som

¹⁰ ICANN RDDS Accuracy Program Specification (<https://www.icann.org/en/system/files/files/registrar-accreditation-agreement-21jan24-en.htm#rdds-accuracy>)

¹¹ [Forordning \(EU\) 2023/1543 om europæiske editions- og sikringskendelser om elektronisk bevismateriale i straffesager og om fuldbyrdelse af frihedsstraffe efter straffesager.](#)

tilsynsmyndigheden skal overveje, når den træffer sine beslutninger. Dette er ikke i overensstemmelse med formålet bag, og indholdet af den kommende forordning.

B. Foreslået alternativ: Medtag proceduremæssige garantier og væsentlige krav til anmodning om oplysninger i overensstemmelse med e-evidensforordningen.

Vi foreslår, at bekendtgørelsen ændres, så den som minimum indeholder de samme sikkerhedsforanstaltninger som e-evidensforordningen:

- Krav om nødvendighed og proportionalitet
- Klar og præcis definition af legitime adgangssøgere – især afklaret, om det kun omfatter danske myndigheder eller også myndigheder fra andre EU-lande og/eller tredjelande.
- Klare topgrænser for bøder
- Retssikkerhed via klageadgang eller domstolsprøvelse

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.

6) Afsluttende bemærkninger

Vi støtter fuldt op om indsatsen for at sikre en sikker, stabil og modstandsdygtig DNS, og vi støtter de overordnede mål i NIS 2-direktivet. Vi anerkender også vigtigheden af at opretholde nøjagtige registreringsdata og behovet for et effektivt samarbejde med de kompetente myndigheder.

Vi mener dog, at det nuværende udkast til bekendtgørelsen indfører forpligtelser, der går ud over, hvad der er nødvendigt for at nå disse mål, og overstiger det niveau for minimumsimplicitering, som den danske lovgiver stræber efter. Dermed risikerer bekendtgørelsen at føre til konkurrenceforvridning, hvor danske forhandlere stilles ringere end deres europæiske modparter.

Den nuværende version af bekendtgørelsen vil i høj grad påvirke registranter af domæner, der administreres via danske forhandlere, da den vil øge priserne, komplicere kunderejsen og føre til en stigning i suspenderingen af legitime domæner.

Der er brug for en mere afbalanceret tilgang - en, der fortsat bidrager til at forebygge og reagere på cyberkriminalitet uden at skabe unødvendige forhindringer for registranter eller for de virksomheder, der betjener dem.

På baggrund af ovenstående opfordrer vi til, at bekendtgørelsen revideres i overensstemmelse med de anbefalinger, der er skitseret i dette brev.

På vegne af

Firmanavn	Navn	E-mailadresse
<i>Danske forhandlere</i>		
group.one checkdomain GmbH one.com A/S - Administrator for .one TLD	Rieke Poppe	rieke.poppe@group.one
team.blue A/S Scannet Wannafind A/S Dandomain A/S Curanet A/S Simply.com A/S register.it S.p.A. Fionia IT ApS Nordicway ApS	Emil Stahl	emil.stahl@team.blue
Onehouse A/S Netsite A/S powerhosting A/S AzeHosting ApS TimeComputer A/S CopenhosA/S e-studio ApS	Dennis Skov Hermannsen Michael Fabricius Bækgaard Storm Thomas Laugesen Christian Reupke Dennis Trabjerg Haiko Schürer Jan Spure Jesper Sandberg Nicolai Christian Bach Frederiksen	dennis@chosting.dk ms@nordicway.dk tgl@onehouse.dk reupke@netsite.dk dt@powerhosting.dk haiko@azehosting.net jan.spure@pro.dk js@copenhosA/S nb@e-studio.dk
MB Solutions A/S Novicell ApS DLX A/S	Bo Melson Julie Oxenvad Karsten Gottenborg Willumsgaard Schmidt	bom@mb-solutions.dk legal@novicell.dk ks@dlx.dk
Mono Solutions ApS NetPlan system design.dk ApS Group Online A/S Web-Koncept A/S Bricksite ApS WNB A/S	Jeppe Rosfeldt Thomas Petersen Dennis Hammer Krogstrup Mike Møller Madsen Jesper Nissen	jr@monosolutions.com thomas@nsd.dk dkr@grouponline.dk mike@bricksite.com jn@wnb.dk
<i>Branche- og interesseorganisationer</i>		
eco – Association of the Internet Industry Registrar Stakeholder Group e.V. (RrSG) Internet Infrastructure Coalition	Lars Steffen Owen Smigelski Christian Dawson	lars.steffen@eco.de owen.smigelski@namecheap.com dawson@i2coalition.com
<i>Registrarforeninger</i>		
Bereas vzw (Belgien) Vereniging van Registrars (Holland) Registrars.se (Sverige)	Bart Mortenmans Berend van Dalfzen Benny Samuelson	info@bereas.be berend@verenigingvanregistrars.nl info@registrars.se

Internationale forhandlere

Miss Group	Frei Leufven	frei@missgroup.com
NameSRS		
Domeneshop AS		
INONOS	Neal McPherson	neal.mcpherson@ionos.dk
InternetX GmbH		
United Domains AG		
Key-Systems GmbH	Volker Greimann	volker.greimann@centralnic.com
Safebrands		
1API GmbH		
Registrygate GmbH		
Tucows Inc	Ashley Renee La Bolle	nicrelations@opensrs.com
ASCIO TECHNOLOGIES, INC. DANMARK		
Namecheap	Hillan Klein	hillan@namecheap.com
Realtime Register B.V.	Theo Geurts	theo.geurts@realtimeregister.com
OVHcloud	Emma Caner	emma.caner@ovhcloud.com
Name.com, Inc.	Beth Marty	beth@identity.digital
Aruba PEC S.p.A	Giorgio Cecconi	giorgio.cecconi@staff.aruba.it
- Administrator for .cloud TLD		
CPS-Datensysteme GmbH	Felix Weigand	few@cps-datensysteme.de
bNamed	Bart Mortelmans	bart@bnamed.net
Hosting Concepts B.V	Arno Vis	avis@openprovider.nl
Scaleway SAS	Cédric Leroy	cleroy@scaleway.com
Webservice	Pascal Nobus	info@webservice.be
Perfect Sence AB (Webb.se)	Jimmy Persson	info@perfectsense.se
Blacknight Internet Solutions Ltd	Michele Neylon	michele@blacknight.com
HostingU2 B.V.	Kasper Martijn Schooneman	kasper@hostingu2.nl
LEMARIT GmbH	Martin Küchenthal	m.kuechenthal@lemarit.com
Abion AB	Jeanett Tesfaledet	jeanett.tesfaledet@abion.com
ingenit GmbH & Co. KG	Jens Meyer	hostmaster@123domain.eu
Excedo Networks AB	Philip Batic	philip.batic@excedo.se
EuroDNS	Lutz Berneke	legal@eurodns.com
Netim	Bruno Vincent	bruno.vincent@netim.com
ISP Service eG	Kurt Jaeger	vorstand@ispeg.de
HolonCom	Robrecht Siera	robrecht.siera@holoncom.eu
Oderland Webbhotell AB	Martin Stenröse	martin.stenrose@oderland.se
101domain GRS Limited	Lauren Tussey	ltussey@101domain.com
Koli-Löks OÜ	Pekka Jalonen	pekka.jalonen@koliloks.eu
managed IP GmbH	Michael Wibbeke	mw@managed-ip.com
DomainMasters BVBA	Ton van der Reijken	ton@domainmasters.be
Lexsynergy Limited	Daniel Greenberg	daniel@lexsynergy.com
Infinite Mho Oy	Atro Tossavainen	atro.tossavainen@infinitemho.fi
Soluciones Corporativas IP, SL	Joan Miquel Durán	jmd@scip.es
Okens Domains	Jerson Jaimes Randazzo	jj@okens.domains
Zone Media OÜ	Ants Korsar	ants@zone.ee
INWX	Mario Peschel	mp@inwx.de
Dotkeeper AB	Marcus Glaad	marcus@dotkeeper.com
Hosting4Real	Lucas Rolff	lucas@perfgrid.com

Andre interessenter

iQ Global AS	Lars Forsberg	lg@iq.global
--------------	---------------	--------------

2025-04-29

Digitaliseringsstyrelsen i Danmark
NIS2@digst.dk

Internetstiftelsens bemærkninger til udkast til bekendtgørelse om validering, verifikation og udlevering af domænenavnsregistreringsdata

Stiftelsen for Internetinfrastruktur ("Internetstiftelsen") ønsker at fremlægge vores synspunkter vedrørende *udkast til bekendtgørelse om validering, verifikation og udlevering af domænenavnsregistreringsdata* (herefter bekendtgørelsen).

Sammenfatning af Internetstiftelsens bemærkninger til udkast til bekendtgørelse

- Et krav om validering og verifikation af både e-mailadresse og telefonnummer ved registrering af domænenavne er et uforholdsmæssigt vidtgående krav for lavrisikodomæner.
- At derudover kræve validering og verifikation af både e-mailadresse og telefonnummer ved hver fornyelse eller årligt er også alt for vidtgående.
- At registranter skal bekræfte deres e-mailadresse og telefonnummer – det vil sige et krav om aktivt svar – med risiko for ellers at blive deaktiveret, er et alt for vidtgående krav.
- Genanvendelse af verifikation af en domæneindehaver bør ligeledes finde anvendelse, når en domæneindehaver har flere domænenregistreringer under forskellige topdomæner.
- Indføres bekendtgørelsen, vil det medføre yderligere byrder og omkostninger for vores registrarer og domæneindehavere, og vi forventer, at mange domæner med korrekte ejeroplysninger vil blive deaktiveret.
- Deaktivering af domænenavne vil i sin tur få store konsekvenser for de involverede parter og udgøre en risiko for stabiliteten på internettet.
- Internetstiftelsen anbefaler en risikobaseret tilgang, hvor registraren får mulighed for at vælge den kontaktform, der fungerer bedst for dem og deres kunder til formålet med verifikation.
- De foreslåede regler indebærer en overimplementering af et allerede vidtgående direktiv, og Internetstiftelsen henstiller til, at Digitaliseringsstyrelsen foretager en grundig gennemgang af konsekvenserne af udkastet og justerer det til en mere formålsbestemt og proportional regulering, inden det kan træde i kraft.

Indledning

Internetstiftelsen har ansvaret for internettets svenske topdomæne .se og varetager desuden driften og administrationen af topdomænet .nu. NIS2-direktivet stiller krav om ensartet anvendelse inden for EU, men implementeres nationalt. Ifølge Internetstiftelsen er det af største vigtighed, at national regulering ikke fører til fragmentering eller uoverensstemmelser mellem medlemsstaternes anvendelse.

22 % af alle .se-domæner og 8 % af alle .nu-domæner er registreret til domæneindehavere i Sverige, men administreres af danske registrarer. På den baggrund må det antages, at bekendtgørelsen, hvis den træder i kraft i sin nuværende form, vil have stor indflydelse på svenske domæneindehavere og den svenske internetinfrastruktur.

Når vi nedenfor skriver registry, henviser det til topdomænenavneadministrator i bekendtgørelsen, og med registrar henvises der til enheder, der leverer domænenavnsregistreringstjenester.

Vedrørende kravet om validering og verifikation af både e-mailadresse og telefonnummer ved registrering (§ 3)

Korrekte registreringsoplysninger er et vigtigt spørgsmål for Internetstiftelsen, og et område vi arbejder aktivt med i samarbejde med vores registrarer. Registries og registrarer i EU arbejder dog efter forskellige modeller, og det er efter Internetstiftelsens opfattelse afgørende, at reguleringer på området tager hensyn til dette.

Som nævnt ovenfor vil bekendtgørelsen, hvis den træder i kraft, berøre et stort antal domæneindehavere i Sverige. Både det svenske topdomæne .se og topdomænet .nu har et højt sikkerhedsniveau. At kræve validering og verifikation af både e-mailadresse og telefonnummer ved registrering under de givne omstændigheder, som foreslået, anses af Internetstiftelsen for at være uforholdsmæssigt vidtgående i forhold til formålet med NIS2-reguleringen, som er at bidrage til sikkerhed, stabilitet og robusthed i DNS.

Internetstiftelsen anbefaler en risikobaseret tilgang, hvor registraren får mulighed for at vælge den kontaktform, der fungerer bedst for dem og deres kunder til formålet med verifikation, hvilket efter vores opfattelse er i overensstemmelse med artikel 28 i NIS2-direktivet.

Vedrørende kravet om validering og verifikation af både e-mailadresse og telefonnummer ved fornyelse eller årligt (§ 3)

At derudover kræve validering og verifikation af både e-mailadresse og telefonnummer ved fornyelse eller årligt, med krav om deaktivering af domæner, hvis domæneindehaveren ikke reagerer, er efter vores opfattelse endnu et eksempel på en alt for vidtgående regulering af et lavrisikodomæne.

Indføres dette krav, vil det medføre yderligere byrder og omkostninger for vores registrarer og domæneindehavere, og vi forventer, at mange domæner med korrekte ejeroplysninger vil blive deaktiveret. Deaktivering af domænenavne vil i sin tur få store konsekvenser for de involverede parter og udgøre en risiko for stabiliteten på internettet.

En deaktivering af et domænenavn påvirker alt indhold under det specifikke domænenavn, for eksempel underliggende sider og e-mailadresser knyttet til domænet. Deaktivering er et meget indgribende tiltag. I sidste ende risikerer et deaktiveret domænenavn at blive permanent afregistreret og derefter frigivet til markedet igen efter "først-til-mølle"-princippet.

Vi har allerede i vores aftaler med registrarer en klausul, der fastslår, at hvis en registrar bliver bekendt med registreringer med forkerte ejeroplysninger, skal vedkommende kontakte domæneindehaveren og kræve, at oplysningerne rettes. Hvis de ikke rettes inden for en vis frist, skal registraren deaktivere domænet. Dette anser vi for at være et rimeligt krav til registrarer som led i en risikobaseret tilgang til at verificere ejerskab, mindske risikoen for falske eller forkerte oplysninger og opnå et højt sikkerhedsniveau.

Vedrørende hvordan verifikation af e-mailadresse og telefonnummer skal gennemføres (§ 3)

Ifølge Internetstiftelsen er kravene i udkastet til bekendtgørelsen om, hvordan e-mailadresse og telefonnummer skal valideres og verificeres, også alt for vidtgående.

Hvis en indehaver skal bekræfte sin e-mailadresse og sit telefonnummer – det vil sige et krav om aktivt svar – risikerer det at føre til et uforholdsmæssigt stort antal deaktiveringer, hvor indehaver overser, at de aktivt skal reagere, eller undlader at gøre det af frygt for, at der er tale om for eksempel phishing.

Vedrørende verifikation af en domæneindehaver med flere domænenavne under samme topdomæne (§ 3, stk. 6)

Internetstiftelsen ser det som positivt, at det tillades at genbruge verifikation af en domæneindehaver til flere domæneregistreringer. Efter vores opfattelse bør dette dog også gælde, når en indehaver har flere domæneregistreringer under forskellige topdomæner – for eksempel topdomænerne .se, .nu, .dk og .com – når de registrerede oplysninger er de samme, og kravene til verifikation ligeledes er de samme.

Afslutning

Internetstiftelsen er engageret i en retssikker, effektiv og proportional implementering af NIS2-direktivet.

De foreslåede regler indebærer en overimplementering af et allerede vidtgående direktiv, hvilket vil medføre yderligere byrder og omkostninger for vores registrarer og domæneindehavere, og vi forventer, at mange domæner med korrekte ejeroplysninger vil blive deaktiveret.

Som nævnt ovenfor medfører deaktivering af domænenavne betydelige konsekvenser for de involverede parter og udgør en risiko for stabiliteten på internettet.

Internetstiftelsen henstiller derfor til, at Digitaliseringsstyrelsen foretager en grundig gennemgang af konsekvenserne af udkastet og justere det til en mere formålsbestemt og proportional regulering, inden det kan træde i kraft.

Vi står til rådighed for dialog om forslaget og dets konsekvenser.

Om Internetstiftelsen

Internetstiftelsen er en uafhængig, erhvervsdrivende og almennyttig organisation. Vi arbejder for et internet, der bidrager positivt til mennesker og samfund.

Vi er en fond, og vores fundats fastslår at vi skal sikre en stærk og sikker infrastruktur for internettet, som opfylder nutidens og fremtidens behov i Sverige, samt fremme forskning, uddannelse og undervisning med fokus på internettet. Vi har ansvaret for internettets svenske topdomæne .se og varetager også drift og administration af topdomænet .nu. Indtægterne fra forretningsdriften finansierer en række initiativer, som har til formål at gøre det muligt for mennesker at bruge internettet på den bedst mulige måde og at formidle viden om brugen af internettet i Sverige samt digitaliseringens indvirkning på samfundet.

Vi tilbyder arrangementer og uddannelsesinitiativer, der gør det lettere at forstå og bruge internettets tjenester, og som bidrager til øget kompetence og flere møder, der fremmer internetinnovation. Vi støtter også forskellige selvstændige opgave- og forskningsprojekter, som på forskellig vis gavner udviklingen af internettet og giver forudsætninger for internetentreprenører og udviklere til at tage skridtet fra idé til færdigt produkt eller tjeneste. Med vores identitetsføderationer forenkler vi login og øger sikkerheden i identitets- og kontohåndtering for både brugere og udbydere af forskellige tjenester inden for skole- og sundhedssektoren.

Vi holder af internettet, tror på det og brænder for at dele vores viden. Vores vision er, at alle i Sverige ønsker, tør og kan bruge internettet.

Sagen er blevet forberedt af Vice President Registry Services Kristian Ørmen samt de seniorjuridiske rådgivere Clara Ludvigsson og Filippa Murath.

For Internetstiftelsen



Carl Piva



NORID DRIVER REGISTERET
FOR NORSKE DOMENENAVN
norid.no

Digitaliseringsstyrelsen i Danmark
NIS2@digst.dk

Deres ref./Your ref.:-

Vår ref./Our ref.: NI:217745

Trondheim, 29. april 2025

Høringssvar til *udkast til bekendtgørelse om validering, verifikasjon og udlevering af domænenavnsregistreringsdata*

Det vises til Digitaliseringsstyrelsens invitasjon til å komme med bemerkninger til *udkast til bekendtgørelse om validering, verifikasjon og udlevering av domænenavnsregistreringsdata* publisert 26. mars 2025 («bekendtgørelsen»).

Om Norid

Norid AS (Norid) er registerenheten («toppdomænenavneadministrator») for de norske landkodedoppdomenene .no (Norge), .sj (Svalbard og Jan Mayen) og .bv (Bouvetøya), og tildeler, administrerer og registrerer domenenavn under disse toppdomenene på grunnlag av overenskomst med den internasjonale forvalter av toppdomener og innenfor rammene av gjeldende rett. Det er kun .no-domenet som er åpent for registrering av domenenavn.

Norids vedtektsfestede formål er å levere sikre og tilgjengelige registrerings- og navnetjenester til internettbrukerne gjennom blant annet å drive navnetjenesten for de norske landkodedoppdomenene på en måte som sikrer god stabilitet og høy teknisk kvalitet. Domenenavnsystemet (DNS) er en grunnleggende funksjon som er helt nødvendig for at internettinfrastrukturen skal fungere. En forutsetning for stabil og robust DNS er at domenenavn som anvendes legitimt og rettmessig, er tilgjengelige, og at disse ikke suspenderes eller slettes unødig. Slik suspensjon eller sletting vil medføre en teknisk fragmentering og uthuling av domenenavnsystemet og dermed dettes robusthet.

For å abonnere på et .no-domene må privatpersoner oppgi navn og fødselsnummer som registrert i det norske Folkeregisteret, og juridiske personer må oppgi organisasjonsnummer som registrert i Brønnøysundregistrene. Det er ikke tillatt å abonnere på .no-domener uten at abonnenten (den som får tildelt bruksretten til et domenenavn - registranten) har et norsk fødselsnummer eller organisasjonsnummer. Norid har med andre ord tildelingsregler med et sterkt nasjonalt (norsk) tilsnitt. Norid er også organisert som et (norsk)statlig eid aksjeselskap og er underlag norske regler, rettsgarantier og håndhevingsmekanismer.

Norid benytter domeneforhandlere (enheter som leverer domenenavnsregistreringstjenester). Selv om Norid stiller krav om at *abonnenten* har nasjonal tilknytning, er Norids praksis at forhandlere av .no skal kunne være etablert både i og utenfor Norge, herunder i Danmark. Dette er en vanlig tilnærming blant registerenheter og underbygger internettets globale karakter.



Forholdet mellom Norid og forhandlerne er regulert gjennom privatrettslige forhandleravtaler som definerer Norids og forhandlerens plikter, rettigheter og ansvar i forbindelse med registrering og administrasjon av domenenavn tildelt av Norid. Forhandlerne har ikke adgang til å suspendere .no-domener i Norids system, og forhandleravtalen setter blant annet skranker for når forhandleren kan slette et domeneabonnement.

Norids syn på NIS2-direktivet, artikkel 28 og nasjonal implementering

Formålet med NIS2-direktivet er å regulere tiltak som skal bidra til et høyt felles nivå av cybersikkerhet på tvers av EU for på denne måten å forbedre hvordan EUs indre marked fungerer (artikkel 1 nr. 1). Selv om NIS2-direktivet er et minimumsdirektiv, er det overordnede formålet fremdeles å sikre en felles standard for cybersikkerhet på tvers av landene.

Ifølge NIS2-direktivet artikkel 2 nr. 12 og 14 og fortalepunkt 14 gjelder forpliktelsene i personvernforordningen («GDPR») uavhengig av reglene i NIS2-direktivet. Det vil si at personvernforordningen gjelder for behandling av personopplysninger som også faller innenfor virkeområdet til NIS2-direktivet. Forpliktelsene etter NIS2-direktivet er ikke ment å innskrenke vernet og forpliktelsene som gjelder for behandling av personopplysninger etter personvernforordningen.

NIS2-direktivet pålegger forpliktelser på medlemsstatene, og direktivet må implementeres i medlemsstatenes nasjonale rett for å forplikte toppdomenenavneadministratorer og enheter som leverer domenenavsregistreringstjenester. Et fellestrekk for mange av forpliktelsene i NIS2-direktivet er at de er utformet på en teknologinøytral måte og foreskriver en risikobasert og proporsjonal tilnærming til hvordan forpliktelsene skal gjennomføres. Dette gjelder blant annet for NIS2-direktivet artikkel 28. Den teknologinøytrale, risikobaserte og proporsjonale tilnærmingen gir pliktsubjektene handlingsrom til å tilpasse tiltakene til hva som egnet og nødvendig for å oppnå formålet med bestemmelsen, og formålet med artikkel 28 er å bidra til DNS' sikkerhet, stabilitet og robusthet («modstandsdygtighet») gjennom å sikre tilgjengeligheten av nøyaktige og fullstendige domenenavnregistreringsdata (artikkel 28 nr. 1).

Verken NIS2-loven § 11 eller bekendtgørelsen henviser uttrykkelig til formålet med NIS2-direktivet artikkel 28. Dette er problematisk. Ikke bare risikerer man at pliktene som oppstilles etter loven § 11 og bekendtgørelsen, tolkes på en måte som ikke er egnet til eller forholdsmessig for å oppnå formålet om å bidra til DNS' sikkerhet, stabilitet og robusthet, men vi mener også at selve bekendtgørelsen inneholder krav som i seg selv er uegnede og uforholdsmessige og i strid med formålet. Norid vil i det følgende redegjøre nærmere for dette synspunktet.

Generelle merknader til bekendtgørelsen

Bekendtgørelsen vil ikke komme direkte til anvendelse for Norid, men vil få indirekte og inngripende betydning for Norid gjennom regulering av forhandlere som har deres hovedforretningssted i Danmark, men forhandler .no-domenenavn til norske kunder. Tilsvarende vil bekendtgørelsen kunne få betydning for andre «toppdomenenavneadministratorer» i andre EU/EØS-medlemsstater og deres forhandlere av domenenavsregistreringstjenester, dersom de har hovedforretningssted i Danmark.

Bekendtgørelsen oppstiller betydelig strengere og mer detaljerte krav enn de som fremgår av NIS2-direktivet artikkel 28. NIS2-direktivet er som nevnt et minimumsdirektiv og er ikke til hinder for en strengere regulering. Når bekendtgørelsen går lengre enn minimumskravene, mister imidlertid pliktsubjektene handlingsrom til å etterleve kravene etter NIS2-loven på en proporsjonal og teknologinøytral måte som står i forhold til og er tilpasset risikoen det enkelte



pliktsubjekt står overfor. Dette er i seg selv problematisk, men utfordringene øker videre gjennom hvordan bekendtgørelsens virkeområde er foreslått regulert.

Det følger av bekendtgørelsen at den gjelder for blant annet enheter «*der leverer topdomænenavnsregistreringstjenester*», uten at dette er begrenset til danske toppdomener. Sammenholdt med NIS2-loven § 2 stk. 2 som sier at «*DNS-tjenesteudbydere, topdomænenavne-administratorer, enheder, der leverer domænenavnsregistreringstjenester og [...] der har deres hovedforretningssted i Danmark, jf. stk. 3, hører under dansk jurisdiktion*», vil bekendtgørelsen vil ha ekstraterritoriell virkning. Dette skyldes at selskaper som har sitt hovedforretningssted i Danmark, også kan være forhandler av domenenavn under landkodetoppdomener i andre land, for eksempel av .no i Norge. Norids tolkning er dermed at selskaper med hovedforretningssted i Danmark som tilbyr registreringstjenester for domenenavn, og som også betjener abonnenter av .no-domener, vil underlegges kravene i den danske NIS2-loven og bekendtgørelsen. Med andre ord, bekendtgørelsen kan ha konsekvenser for .no-domeneabonnenter basert på at deres domeneforhandler opererer fra Danmark.

Kravene i bekendtgørelsen om validering, verifikasjon og utlevering vil være svært utfordrende for forhandlerne, som risikerer å bryte avtalen med Norid, eventuelt også krav de er underlagt i andre jurisdiksjoner, dersom de etterlever de strenge kravene i bekendtgørelsen. De vil også stå overfor vanskeligere markedsvilkår enn deres konkurrenter som ikke underlegges like strenge krav som bekendtgørelsen. Den ekstraterritoriale virkningen er også en byrde for abonnenten, som risikerer å få sitt domenenavn suspendert eller slettet og å få deres personopplysninger utlevert i flere tilfeller enn de som følger av NIS2-direktivets minimumsregulering. At bekendtgørelsen går lengre enn minimumskravene i NIS2-direktivet, vil kunne oppmuntre til «forum shopping» både fra abonnentenes og forhandlerens side. I ytterste konsekvens må Norid overveie sitt fremtidige samarbeid med forhandlere som er underlagt bekendtgørelsens strenge krav - dersom disse forhandlerne ikke kan overholde forhandleravtalen.

Norid må også ivareta abonnentenes interesser i tråd med gjeldende norske krav. Hensynet til abonnentenes personvern og de grunnleggende personvernprinsippene i GDPR er ikke tilstrekkelig ivaretatt i bekendtgørelsen. Behandling av personopplysninger og EUs databeskyttelseslovgivning er uttrykkelig henvist til i NIS2-direktivet artikkel 28 nr. 1, 4 og 5. Vi kan imidlertid ikke se at sentrale personvernprinsipper slik som dataminimering og forholdsmessighet er hensyntatt i forbindelse med bekendtgørelsens bestemmelser, herunder ved utformingen av bestemmelsen om hasteanmodninger. Viktigheten av disse prinsippene støttes også av fortalepunkt 111, som fremhever at prosedyrene for verifisering må være proporsjonale.

Det er svært betenkelig at bekendtgørelsen ikke henviser til det uttalte formålet med NIS2-direktivet artikkel 28 om å styrke DNS' sikkerhet, stabilitet og motstandsdyktighet. Bestemmelsene i bekendtgørelsen tar heller ikke hensyn til den proporsjonale, risikobaserte og teknologinøytrale reguleringen som NIS2-direktivet artikkel 28 legger opp til. Et rigid og snevert handlingsrom for forhandlerne til å implementere kravene i bekendtgørelsen, kan i verste fall føre til at mange legitime og lovlige abonnenters domener blir suspendert og slettet som følge av formaliteter. Dette kan igjen påvirke DNS' stabilitet og motstandsdyktighet negativt - stikk i strid med formålet med NIS2-direktivet artikkel 28.

I forlengelsen av disse hovedpunktene vil vi knytte noen merknader til enkelte av bestemmelsene i bekendtgørelsen.



Anvendelsesområde (§ 1)

Enheter som leverer domenenavnsregistreringstjenester, og som også er domeneforhandlere i Norge, kan som nevnt bli underlagt dansk jurisdiksjon gjennom den foreslåtte bekendtgørelsen. Når domeneforhandlere med hovedforretningssted i Danmark også er forhandlere av .no-domenenavn, vil de strengere og mer detaljerte kravene i bekendtgørelsen legge føringer for avtaleforholdet mellom forhandleren og den norske domeneabonnenten. I neste rekke påvirker dette avtaleforholdet mellom Norid og abonnenten, for eksempel dersom bekendtgørelsen krever at en forhandler suspenderer eller sletter et abonnement i tilfeller der forhandler ikke kan suspendere domenenavnet og sletting ikke er berettiget etter avtalevilkårene som gjelder mellom Norid og abonnenten. Det er problematisk at bekendtgørelsen går så langt utenfor minimumsreguleringen i et grensekryssende marked.

Kravet til verifikasjon av både telefonnummer og e-postadresse ved registrering (§ 3)

Bekendtgørelsen går lenger enn det artikkel 28 i NIS2-direktivet krever hva gjelder verifikasjon av kontaktinformasjon. Et ubetinget krav til verifisering av to kontaktmetoder (telefonnummer og e-postadresse) kan ikke anses nødvendig for å oppnå formålet med registreringsplikten og er heller ikke forholdsmessig. Det bemerkes at det på nåværende tidspunkt ikke er et krav om å samle inn telefonnummer fra abonnenter etter norsk rett. Norid mener dessuten det er tilstrekkelig etter NIS2-direktivet artikkel 28 å kun samle inn én form for kontaktinformasjon, det som er nødvendig for å kontakte abonnenten. Kravet i bekendtgørelsen vil derimot både kreve innsamling av en ytterligere kontaktmetode for alle berørte norske abonnenter, og verifisering av denne informasjonen.

Norid stiller også spørsmål ved om krav til verifisering av både e-postadresse og telefonnummer i bekendtgørelsen har hjemmel. Et krav om å verifisere både telefonnummer og e-postadresse har ikke forankring i ordlyden i NIS2-direktivet artikkel 28 - tvert imot tilsier NIS2-direktivet fortalespunkt 111 at verifisering av én kontaktmetode er tilstrekkelig - og fortalespunktet dikterer heller ikke hvilken av kontaktmetodene som må verifiseres. Det vises også til uttalelsene fra Punktum dk vedrørende at forslaget om dobbel verifisering går utenfor rammene av det som er hjemlet i NIS2-loven § 11 stk. 3. Kravet til dobbel verifisering strider også mot dataminimeringsprinsippet i GDPR.

Bekendtgørelsen burde heller åpnet for vurderinger fra pliktsubjektets side vedrørende verifikasjon for å sikre en risikobasert og proporsjonal tilnærming.

Hva som kreves av verifikasjonen (§ 3)

Bekendtgørelsen oppstiller unødig detaljerte tekniske krav til verifikasjonen. NIS2-direktivet artikkel 28 er formulert på en teknologinøytral måte. Dette er en styrke fordi det åpner for å velge en metode som er tilpasset den teknologiske utviklingen til enhver tid, samt risikoene og den faktiske situasjonen pliktsubjektet står overfor. Ved å diktere en bestemt teknisk fremgangsmåte låser man seg til et bilde av teknologien og risikoen på ett tidspunkt. For å sikre en risikobasert og proporsjonal tilnærming, slik direktivet foreskriver, bør det legges opp til at toppdomenenavneadministratorer og leverandører av domenenavnsregistreringstjenester får mulighet til å gjøre flere uavhengige vurderinger.

Videre byr kravet i bekendtgørelsen om bruk av telefonnummer formatert etter ITU-T E.164s standarder for internasjonale telefonnumre på utfordringer. Dette kravet innebærer at alle abonnenter må bruke et nummer som overholder den relevante nasjonale nummerplanen for at valideringen av domenenavn skal anses som gyldig. Dette kan komme i konflikt med tilgjengelighetskrav fastsatt i europeisk og nasjonal lovgivning utenfor Danmark.



Suspensjon eller sletting ved manglende verifikasjon (§ 5)

Å oppstille et krav om at domenenavnet slettes ved manglende verifikasjon av både e-post og telefonnummer, er uforholdsmessig byrdefullt og kan føre til store konsekvenser for forhandlerne, registerenhetene og ikke minst abonnentene. Det er åpenbart at det store flertallet av abonnenter er legitime og benytter sitt domeneabonnement på lovlig vis. Strengt krav til verifisering hvor abonnenten risikerer suspensjon eller sletting, er svært inngripende overfor en så stor gruppe individer og virksomheter.

Formålet med NIS2-direktivet artikkel 28 om å sikre felles robusthet for DNS kan neppe sies å ivaretas på en god måte dersom tusentalls av legitime abonnenter risikerer å miste sine domeneabonnement med mindre de følger strenge og rigide verifikasjonsprosedyrer, særlig dersom de må bekrefte informasjon **både** via e-post **og** telefonnummer. Dette gjelder med styrke i en tid hvor mange abonnenter - med rette - er bekymret for phishing, svindel og lignende angrep nettopp via e-post og telefon. Bestemmelsen vil kunne ha alvorlige og utilsiktede konsekvenser for abonnenter - både privatpersoner og virksomheter - som har et legitimt behov for å opprettholde sitt domeneabonnement.

Bekendtgørelsen burde i stedet gitt pliktsubjektene større handlingsrom for å vurdere om suspensjon eller sletting er et proporsjonalt tiltak avhengig av risikoen i det enkelte tilfellet.

Hasteanmodninger om adgang til domenenavnsregistreringsdata (§ 6)

I bekendtgørelsens § 6 er det gitt adgang til å be om spesifikke domenenavnsregistreringsdata innen 24 timer, såkalte hasteanmodninger. Vi kan ikke se at denne strengere fristen har klar hjemmel verken i NIS2-loven eller NIS2-direktivet. Også her viser vi til uttalelsene fra Punktum dk om at utlevering av opplysninger innen 24 timer går ut over rammene for det som er hjemlet i NIS2-loven. En slik strengere regulering vil også kunne få store konsekvenser for tusenvis av abonnenter på .no-domener - herunder personvernkonsekvenser - ettersom danske forhandlere kan få en utleveringsplikt for personopplysninger om norske individer uten at disse ekstraterritorielle virkningene er hensyntatt.

Norid vil påpeke at flere av hastetilfellene nevnt i § 2 vil innebære behandling av særlige kategorier av personopplysninger eller opplysninger om straffedommer og lovovertridelser. Dette krever et ekstraordinært behandlingsgrunnlag etter personvernforordningen artikkel 9 nr. 2 og artikkel 10, noe som også synes å være oversett i utformingen av bekendtgørelsen.

Oppsummeringsvis mener Norid at bekendtgørelsen går for detaljert til verks og gir en alt for streng regulering sammenlignet med handlingsrommet og tilnærmingen i NIS2-direktivet. Flere av bekendtgørelsens bestemmelser er uforholdsmessig inngripende og hensyntar ikke formålet som ligger til grunn for NIS2-direktivet artikkel 28, herunder DNS' robusthet. Bekendtgørelsens bestemmelser har ekstraterritoriell virkning og griper inn i Norids virksomhet, forhandlerens virksomhet, avtaleforholdet med abonnentene og abonnentenes interesser, herunder deres personvern. Bekendtgørelsen burde i større grad åpnet for en proporsjonal, teknologinøytral og risikobasert tilnærming.



For øvrig støtter Norid merknadene i høringsinnspillene fra Punktum dk, Internettstiftelsen og fellesuttalelsene fra One.com med flere («registrars»).

Vennlig hilsen
Norid AS

Hilde Thunem
Administrerende direktør

Ann-Cathrin Marcussen
Avdelingsleder Tjeneste / Head of Legal

Til: Digitaliseringsstyrelsen

Vedr.: Høringssvar til udkast til bekendtgørelse om validering, verifikation og udlevering af domænenavnsregistreringsdata

Kære Digitaliseringsstyrelsen

Vi takker for muligheden for at kommentere udkastet til bekendtgørelse vedrørende domænenavnsregistreringsdata.

De foreslåede krav vækker alvorlig bekymring hos **One Registry**, særligt på grund af omfanget og den tekniske implementering. Forpligtelserne vedrørende verifikation af både e-mail og telefonnummer, krav om verifikation før aktivering af domæner samt gentagelse af verifikation ved fornyelse skaber betydelige praktiske og juridiske barrierer for os som danskrevet global gTLD-administrator.

Om .one

.one er det eneste åbne generiske topdomæne (gTLD), der drives af en dansk virksomhed. Vi administrerer cirka 270.000 aktive domænenavne, hvoraf størstedelen er registreret uden for Danmark, herunder en stor andel i USA.

Som gTLD opererer **.one** inden for den internationale kontraktlige ramme etableret af ICANN. Vi arbejder udelukkende gennem et globalt netværk af akkrediterede forhandlere, der sælger domænenavne direkte til slutbrugere.

Implementering er ikke teknisk eller kontraktuelt mulig

gTLD-administratorer som os er hverken teknisk eller kontraktuelt i stand til at opfylde bekendtgørelsens krav, da vores rolle som administrator og afhængighed af ikke-danske forhandlere - både til salg og teknisk drift - sætter klare begrænsninger:

- **Vi har ikke direkte kontakt med registranter**

Det er forhandlerne, der har den direkte relation til registranten og som normalt står for dataindsamling og -verifikation. Dette gælder for alle gTLD'er og de fleste ccTLD'er.

Hvis vi skulle designe og implementere et verifikationssystem for .one-registranter, ville det potentielt komme i konflikt med forhandlerne egne processer og sandsynligvis føre til overdreven og dobbelt dataindsamling. Derudover vil det føre til, at legitime hjemmesider bliver suspenderet, da registranterne ikke kender os og derfor med rette kan være skeptiske overfor en e-mail, der beder om ID-verifikation. Omkring 30 % af .one-registranterne er amerikanske statsborgere, som ikke er vant til denne form for omfattende KYC.

- **De fleste af vores forhandlere er ikke underlagt dansk lovgivning**
Størstedelen af vores forhandlere er baseret uden for Danmark og skal følge lovgivningen i deres hjemland. Danmark er p.t. det eneste EU-land, der pålægger så omfattende verifikationskrav.
Et krav om, at ikke-danske forhandlere skal implementere danske regler, vil føre til, at de stopper salget af .one-domæner, da de ikke vil indføre særligt byrdefulde KYC-processer for et relativt lille TLD.
- **Vores backend drives af en tredjepartsleverandør, som ikke understøtter landespecifikke verifikationsmekanismer**
Vores tekniske backend-leverandør vil ikke tilpasse sin løsning for et enkelt lille TLD som .one. Det vil ikke være kommercielt bæredygtigt for dem.

Som et åbent gTLD under ICANN og som del af et globalt økosystem har vi meget begrænsede muligheder for ensidigt at pålægge vores forhandlere nye verifikationskrav. Disse begrænsninger gør det umuligt for **One Registry** at opfylde de foreslåede forpligtelser i bekendtgørelsen.

Forslag til fremgangsmåde

Vi anbefaler, at bekendtgørelsen begrænses til en minimumsimplicitering af NIS 2-direktivet. Det vil sikre, at Danmark ikke indfører strengere krav end andre EU-lande. Alle forhandlere, som er baseret i eller tilbyder tjenester i EU, vil være forpligtet til at følge de fælles minimumskrav i direktivet. Sammen med vores forhandlere kan **One Registry** sikre overholdelse af disse krav – men vi kan ikke pålægge vores forhandlere strengere verifikationskrav end dem.

Vi foreslår derfor følgende ændringer for at bringe bekendtgørelsen i overensstemmelse med andre EU-lande og de anbefalinger, der fremgår af direktivet:

- Kun kræve verifikation af én kontaktmetode (e-mail *eller* telefon), ikke begge.
- Tillade, at domæner aktiveres før verifikation, så længe den gennemføres indenfor en rimelig frist.
- Fjerne kravet om at gentage verifikation ved fornyelse, medmindre data er ændret, eller der er berettiget tvivl om korrekthed.
- Tillade genbrug af verificerede oplysninger, når registranter registrerer flere domæner med samme data.
- Indføre klare, proportionalitetsbaserede regler for udlevering af registreringsdata til tredjepart.
- Definere tydeligt, hvad der forstås ved "legitime adgangssøgere", og om disse kun omfatter danske myndigheder eller også udenlandske, samt under hvilke betingelser en anmodning anses som "legitim".

Afsluttende bemærkninger

Vi er stolte af at drive et internationalt anerkendt TLD fra Danmark og støtter ambitionen om at styrke sikkerhed, pålidelighed og modstandsdygtighed i domænesystemet. Men uden justeringer vil bekendtgørelsen pålægge uforholdsmæssige byrder på danske gTLD-administratorer og skade Danmarks position i det internationale domæneøkosystem.

Som det ser ud nu, vil det ikke være muligt at fortsætte driften af **One Registry** under de foreslåede regler, da vores forhandlere ikke vil kunne støtte os. I sidste ende kan det tvinge os til at flytte driften til en mere lempelig jurisdiktion uden for Danmark.

Vi anmoder derfor om, at bekendtgørelsen revideres, så den afspejler internationale best practices og en minimumsimplementering af NIS 2-direktivet.

Digitaliseringsstyrelsen
Att. Finn Petersen

Sendt pr. mail til NIS2@digst.dk

København, den 29. april 2025

Høring over udkast til bekendtgørelse om validering, verifikation og udlevering af domænenavnsregistrerings-data

Bemærkninger til bekendtgørelse

RettighedsAlliancen vil hermed komme med sine bemærkninger til høringsbrev af 26. marts 2025 fra Digitaliseringsstyrelsen vedrørende udkast til bekendtgørelse om validering, verifikation og udlevering af domænenavnsregistrering-data, som forventes at træde i kraft den 1. juli 2025 sammen med lovforslaget L 141 (NIS 2-loven).

RettighedsAlliancen vil indledningsvist bifalde initiativer, der har til formål at øge internetsikkerheden gennem krav til topdomæneadministratorer og enheder, der leverer domænenavnsregistreringstjenester for at styrke validerings- og verifikationsmetoder.

RettighedsAlliancen bemærker, at bekendtgørelsen ikke eksplicit sonder mellem danske og udenlandske registranter. Ifølge § 4 skal der ved registrering af et domænenavn "*i det omfang der er mulighed for det*" anvendes "*elektronisk identifikation til at verificere en registrants navn*", dvs. personidentifikationsdata i elektronisk form, der entydigt repræsenterer enten en juridisk eller en fysisk person, der repræsenterer en juridisk person, jf. bekendtgørelsens § 2, nr. 4.

Det fastslås videre i § 4, stk. 2, at hvis elektronisk identifikation ikke er mulig ved verificering af registrantens navn, anvendes i stedet en risikobaseret tilgang baseret på bedste praksis. Efter de nugældende regler, verificeres danske registranter som udgangspunkt ved elektronisk ID-kontrol via MitID, mens udenlandske registranter vurderes ud fra en risikobaseret tilgang. Bekendtgørelsen medfører således ikke et

stærkere grundlag for kontrol sammenlignet med den nuværende retstilstand. RettighedsAlliancen har på baggrund af sit kendskab til området erfaret, at denne risikobaserede vurdering ikke er tilstrækkelig for at forhindre misbrug.

RettighedsAlliancen har konstateret en stigende tendens til, at .dk-domæner anvendes til bl.a. ulovlig distribution af kopivarer og udbud af IPTV-tjenester. Udbredelsen af AI-værktøjer bidrager generelt til en stigning i online rettighedskrænkelser, som i øvrigt ofte kan være vanskelige for internetbrugere at identificere. Disse ulovlige sider er oftest registreret af udenlandske registranter.

På den baggrund opfordrer RettighedsAlliancen til en skærpet kontrol med udenlandske registranter, navnlig i forbindelse med beskyttelsen af .dk-domænets troværdighed og for at sikre, at domæner ikke misbruges til ulovlige aktiviteter.

Konkret foreslås det, at kravene til udenlandske registranter eksplicit skærpes i forhold til danske registranter, og at udenlandske registranter skal opgive ID-dokumentation, så domænet først aktiveres efter verificering af den udenlandske registrant på linje med den verifikationsproces, der gør sig gældende for danske registranter, som anvender MitID.

RettighedsAlliancen støtter bekendtgørelsens § 5, der forudsætter, at et domæne først aktiveres, når verificering af e-mail, telefonnummer og registrantens navn er gennemført med et tilfredsstillende resultat. Ligeledes bifaldes § 6, som sikrer adgang til specifikke registreringsdata inden for 72 timer efter en begrundet anmodning fra en legitim adgangssøger.

RettighedsAlliancen opfordrer dog i forlængelse af § 5 til en udvidelse, så 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, f.eks. i tilfælde af åbenbare rettighedskrænkelser.

København, den 29. april 2025

Maria Fredenslund
Direktør, RettighedsAlliancen

T: +45 21647448

M: maria.fredenslund@rettighedsalliancen.dk