

Bekendtgørelse om validering, verifikation og udlevering af domænenavsregistreringsdata¹⁾

I medfør af § 11, stk. 8, og § 32, stk. 3, i lov nr. 434 af 6. maj 2025 om foranstaltninger til sikring af et højt cybersikkerhedsniveau (NIS 2-loven) fastsættes:

Anvendelsesområde og definitioner

§ 1. Denne bekendtgørelse finder anvendelse på topdomænenavneadministratorer og enheder, der leverer domænenavsregistreringstjenester, som er omfattet af NIS 2-loven.

§ 2. I denne bekendtgørelse forstås ved:

- 1) Syntaktisk validering: En sikring af, at data er korrekt formateret på tværs af indtastningsfelter.
- 2) Operationel verifikation: En sikring af, at indsamlede kontaktoplysninger er funktionelle og muliggør kontakt.
- 3) Identitetsverifikation: Indsamling og validering af information om en registrant for at sikre, at registranten er den, som registranten udgiver sig for at være.
- 4) Elektronisk identifikation: Personidentifikationsdata i elektronisk form, der entydigt repræsenterer enten en fysisk eller juridisk person eller en fysisk person, der repræsenterer en juridisk person.
- 5) Kontaktpunkt: En fysisk eller juridisk person, som har fået overdraget ansvaret fra en registrant til at administrere et domænenavn på registrantens vegne, og som kan udføre alle handlinger vedrørende et domænenavn, herunder ændre i domænenavsregistreringsdata, foretage fornyelse af domænenavnet eller overføre domænenavnet til en anden part.
- 6) DNS-misbrug: Det at et domænenavn anvendes som en del af et botnet, anvendes til phishing eller pharming, eller anvendes til at sprede malware eller spam, når spam fungerer som en leveringsmekanisme for botnet, phishing eller pharming.
- 7) Legitime adgangssøgende: En fysisk eller juridisk person, der fremsætter en anmodning i henhold til EU-retten eller national ret om at få adgang til ikke-offentligt tilgængelige domænenavsregistreringsdata, herunder personoplysninger.

Validerings- og verifikationsprocedurer for e-mailadresse eller telefonnummer

§ 3. Ved registrering af et domænenavn skal topdomænenavneadministratorer og enheder, der leverer domænenavsregistreringstjenester, sikre, at registrantens kontakt-e-mailadresse eller telefonnummer er syntaktisk valideret og operationelt verificeret i medfør af stk. 4, jf. dog stk. 5.

Stk. 2. Hvis registranten på registreringstidspunktet har et kontaktpunkt, eller på et senere tidspunkt etablerer et kontaktpunkt, der administrerer domænenavnet, skal der ved registrering af et domænenavn, ved registrering af et kontaktpunkt eller ved ændring af et eksisterende kontaktpunkts kontaktoplysninger, gennemføres en syntaktisk validering og en operationel verificering efter stk. 4 for kontakt-e-mailadressen eller telefonnummeret for kontaktpunktet i tilfælde af, at de er forskellige fra registrantens kontakt-e-mailadresse eller telefonnummer.

Stk. 3. Den syntaktiske validering og operationelle verificering efter stk. 1 skal også udføres, hvis

- 1) et domænenavn overføres til en anden registrant,
- 2) topdomænenavneadministratoren eller enheden, der leverer domænenavsregistreringstjenester, modtager en skriftlig begrundet mistanke om, at et domænenavn anvendes i forbindelse med DNS-misbrug, eller
- 3) topdomænenavneadministratoren eller enheden, der leverer domænenavsregistreringstjenester, modtager en skriftlig begrundet mistanke om, at kontaktoplysninger for et domænenavn ikke er korrekte.

Stk. 4. Den syntaktiske validering og operationelle verifikation skal mindst omfatte en af følgende

- 1) at e-mailadressen er formateret i overensstemmelse med RFC5322 (eller senere standarder, som træder i stedet for), og er operationelt verificeret eller
- 2) at telefonnummeret er formateret i overensstemmelse med ITU-T E 164's anbefalinger for internationale telefonnumre, og er operationelt verificeret.

Stk. 5. Hvis en registrant registrerer eller har registreret flere domænenavne hos samme enhed, er det tilstrækkeligt at udføre den syntaktiske validering og operationelle verificering af registrantens kontakt-e-mailadresse eller telefonnummer efter stk. 1 for ét af registrantens domænenavne.

Verifikationsprocedurer af registrantens navn

§ 4. Ved registrering af et domænenavn skal topdomænenavneadministratorer og enheder, der leverer domænenavnsregistreringstjenester, i det omfang der er mulighed for det, anvende elektronisk identifikation til at verificere en registrants navn, jf. dog stk. 2 og 6.

Stk. 2. Hvis en topdomænenavneadministrator og en enhed, der leverer domænenavnsregistreringstjenester, ikke har mulighed for at anvende elektronisk identifikation til at verificere en registrants navn, anvendes i stedet en risikobaseret tilgang. Den risikobaserede tilgang skal tage hensyn til bedste praksis på området.

Stk. 3. Den risikobaserede tilgang anvendes ved registrering af et domænenavn og ved hver fornyelse af et eksisterende domænenavn.

Stk. 4. Hvis den risikobaserede tilgang viser, at en registrering udgør en medium eller høj risiko for at blive anvendt i ondsindet øjemed, skal topdomænenavneadministratoren og enheden, der leverer domænenavnsregistreringstjenester, gennemføre en identitetsverifikation af registranten.

Stk. 5. Verifikation af en registrants navn efter stk. 1 eller 2 skal også udføres, hvis

- 1) et domænenavn overføres til en anden registrant,
- 2) topdomænenavneadministratoren eller enheden, der leverer domænenavnsregistreringstjenester, modtager en skriftlig begrundet mistanke om, at et domænenavn anvendes i forbindelse med DNS-misbrug, eller
- 3) topdomænenavneadministratoren eller enheden, der leverer domænenavnsregistreringstjenester, modtager en skriftlig begrundet mistanke om, at kontaktoplysninger for et domænenavn ikke er korrekte.

Stk. 6. Hvis en registrant registrerer eller har registreret flere domænenavne hos samme enhed, er det tilstrækkeligt at anvende elektronisk identifikation til at verificere registrantens navn efter stk. 1 for ét af registrantens domænenavne eller at anvende den risikobaserede tilgang til at verificere registrantens navn efter stk. 2 for ét af registrantens domænenavne.

Manglende validering eller verifikation af domænenavnsregistreringsdata

§ 5. Hvis kontakt-e-mailadressen eller telefonnummeret for registranten af et domænenavn eller et eventuelt kontaktpunkt ikke kan valideres syntaktisk og verificeres operationelt, jf. § 3, stk. 1 og 2, eller hvis navnet på registranten ikke kan verificeres, jf. § 4, stk. 1 og 2, kan domænenavnet først gøres aktivt, når validering og verificering af kontakt-e-mailadresse eller telefonnummer samt verificeringen af navnet på registranten er gennemført med et tilfredsstillende resultat, jf. dog stk. 2.

Stk. 2. I tilfælde, hvor det ikke er teknisk muligt at foretage validering og verifikation efter bestemmelserne i §§ 3 og 4, før domænenavnet gøres aktivt, skal tilfredsstillende validering og verificering af kontakt-e-mailadresse eller telefonnummer samt verificering af navnet på registranten ske senest 72 timer efter domænenavnet er gjort aktivt. Sker der ikke tilfredsstillende validering og verificering inden for 72 timer, skal domænenavnet uden ugrundet ophold suspenderes eller slettes.

Stk. 3. I situationer omfattet af § 3, stk. 3, § 4, stk. 5, eller fornyelser efter § 4, stk. 3, skal domænenavnet suspenderes eller slettes inden for 30 dage, hvis ikke validering og verificering kan ske forinden på baggrund af opdaterede oplysninger fra registranten.

Anmodninger om adgang til domænenavnsregistreringsdata

§ 6. Topdomænenavneadministratorer og enheder, der leverer domænenavnsregistreringstjenester, skal på baggrund af en lovlig og behørigt begrundet anmodning fra en legitim adgangssøger give adgang til de anmodede specifikke domænenavnsregistreringsdata uden unødigt ophold og under alle omstændigheder inden for 72 timer.

Stk. 2. For øvrige adgangssøgende skal topdomænenavneadministratorer og enheder, der leverer domænenavnsregistreringstjenester, på baggrund af en behørigt begrundet anmodning om adgang til specifikke ikke-offentliggjorte domænenavnsregistreringsdata inden for 72 timer efter modtagelse af anmodningen oplyse, om adgang gives til de domænenavnsregistreringsdata, som anmodningen vedrører.

Stk. 3. Hvis en anmodning efter stk. 2 hverken helt eller delvist imødekommes, medsender topdomænenavneadministratorer eller enheder, der leverer domænenavnsregistreringstjenester, en begrundelse herfor.

Påbud

§ 7. Der kan meddeles påbud til topdomænenavneadministratorer og enheder, der leverer domænenavnsregistreringstjenester, med henblik på at sikre overholdelse af §§ 3-6.

Straffebestemmelser

§ 8. Med bøde straffes den, der

- 1) overtræder § 3, stk. 1-4, § 4, stk. 1-5, § 5 eller § 6, eller
- 2) undlader at efterkomme påbud efter § 7.

Stk. 2. Der kan pålægges selskaber m.v. (juridiske personer) strafansvar efter reglerne i straffelovens 5. kapitel.

Ikrafttrædelse

§ 9. Bekendtgørelsen træder i kraft den 1. januar 2026.

Digitaliseringsministeriet, den 4. juni 2025

CAROLINE STAGE OLSEN

/ Tanja Franck

- ¹⁾ Bekendtgørelsen gennemfører dele af Europa-Parlamentets og Rådets direktiv (EU) 2022/2555 af 14. december 2022 om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen, om ændring af forordning (EU) nr. 910/2014 og direktiv (EU) 2018/1972 og om ophævelse af direktiv (EU) 2016/1148 (NIS 2-direktivet), EU-Tidende 2022, nr. L 333, side 80.