

manitu GmbH, Welvertstraße 2, 66606 St. Wendel, Deutschland

Deutscher Bundestag
Ausschuss für Inneres und Heimat
An alle Mitglieder
Platz der Republik 1
11011 Berlin

Deutscher Bundestag

Ausschuss für Inneres und Heimat

Ausschussdrucksache
20(4)516

Ihr Zeichen / Ihre Nachricht vom

Unsere Zeichen / Unsere Nachricht vom

Datum

15.10.2024

Stellungnahme zum aktuellen Stand des Gesetzgebungsverfahrens zur NIS-2-Richtlinie

Sehr geehrte Damen und Herren,

wir nehmen hiermit als betroffene Einrichtung Stellung zum aktuellen Stand des Gesetzgebungsverfahrens zur NIS-2-Richtlinie, insbesondere

- a) zur Stellungnahme des Bundesrats vom 27.09.2024 in der 1047. Sitzung (Drucksache 380/24)
- b) zu § 49 des aktuellen Entwurfs
- c) zu § 50 des aktuellen Entwurfs

ad a) Stellungnahme des Bundesrats bzgl. Bekämpfung von Fake-Shops

Wir lehnen in Einklang mit der Bundesregierung (siehe Anlage 5 der Drucksache 20/13184) die Vorschläge und Forderungen des Bundesrats in Bezug auf Bekämpfung von Fake-Shops und die geforderte Verifikation von Domain-Inhabern vollumfänglich ab.

Eine solche verpflichtende Verifikation von Domain-Inhabern führt – wenn nur in Deutschland oder auch nur in Europa eingeführt – letztendlich zu einer schlechteren Sicherheit für Endverbraucher.

Denn: Eine solche Maßnahme wäre erst einmal nur auf Deutschland oder maximal Europa beschränkt. Betreiber von Fake-Shops würden dann ohne Aufwand im Ausland Domains registrieren – dort ohne Verifikation. Die Endnutzer

würden jedoch erwarten, dass Domains „verifiziert“ sind und sich genau deshalb künftig darauf verlassen, ohne kritisch zu hinterfragen – und dann in die „Falle“ tappen.

Darüber hinaus weisen wir darauf hin, dass eine solche Verifikation bei einem Massengeschäft (es werden täglich mehrere Millionen Domains registriert) faktisch nicht machbar ist. Eine Domain-Registrierung hat oft nur Margen im Bereich weniger Cent (!). Eine Verifikation ist ein personeller Aufwand, der mit 15 bis 30 Minuten anzusetzen ist. Die Kosten müssten die Verbraucher tragen. **Das würde letztendlich das Geschäft in Deutschland für Domains fast vollumfänglich zerstören und damit den Umsatz und Arbeitsplätze schlicht ins Ausland (vermutlich sogar außerhalb der EU) verlagern** – was aufgrund der reinen Online-Dienstleistung nur eine Verlagerung des Firmensitzes nötig macht.

ad b) § 49 des aktuellen Entwurfs

Der aktuelle Entwurf sieht in § 49 Sorgfaltspflichten für Anbieter vor, die in eine ähnliche Richtung wie ebd. gehen.

Darin sind einige Punkte enthalten, die praxisfern und wirtschaftsfeindlich sind:

1. Es fehlt eine Konkretisierung, was „gebotene Sorgfalt“ nach Abs. 1 bedeutet. Dies ist dehn- und auslegbar und bedeutet in der Auseinandersetzung mit Aufsichtsbehörden Potential für Streitigkeiten.
2. Der Zwang nach einer Telefon-Nummer des Nutzers einer Domain wird in der Praxis immer zu Problemen führen, denn gerade Endverbraucher geben diese Daten nur ungern (aus Gründen des „Datenschutzes“) weiter. Letztendlich wird in der Praxis von Kunden oft eine Fake-Telefonnummer angegeben werden. Für nicht-natürliche Personen ist die Telefonnummer sowieso praxisfern, denn was bringt die Telefon-Zentrale eines großen Konzerns als „Kontaktstelle“, wenn dort niemand erreicht werden kann?
3. Der Passus „anhand derer (...) Inhaber (...) identifiziert (...) werden können“ im Abs. 2 birgt Potential für Streitigkeiten mit Aufsichtsbehörden. Gerade wenn es sich bei Domain-Inhabern um nicht-natürliche Personen handelt, ist eine „Identifikation“ in der Praxis realitätsfern. Wie soll man eine Aktiengesellschaft identifizieren? Oder den Gesellschafter-Geschäftsführer einer GmbH? Man wird kaum erwarten können, dass die handelnden Personen für eine solche „Verifikation“ stets persönlich zur Verfügung stehen.
4. Die Verpflichtung nach Abs 3., Verfahren zu etablieren, die die Informationen in der Datenbank sicherstellen, und deren Pflicht zur Offenlegung sind mehr als realitätsfern. Wenn solche Verfahren öffentlich werden, wäre dies eine Einladung an Betrüger, genau diese Verfahren zu umgehen. Wenn es solche Verfahren geben soll, sollte die

zuständige Behörde diese für alle Anbieter gleichlautend definieren und z.B. als BSI-Richtlinie vorgeben. Diese Pflicht jedem Anbieter aufzuerlegen, ist unzumutbar.

ad b) § 50 des aktuellen Entwurfs

Die Verpflichtung, Informationen nach Abs. 1 innerhalb von 72 Stunden (3 Tagen!) nach Eingang eines Antrags zugänglich zu machen, führt faktisch zu einer Verpflichtung eines 24x7-Betriebes. Im aktuellen Gesetzesentwurf steht „Stunden“ und nicht „Tage“ und erst recht nicht „Werktage“.

Es ist uns kein anderer Rechtsweg im ordentlichen Rechtsverfahren bekannt, das derart kurze Fristen vorsieht. Selbst Anordnungen von Gerichten, Bescheide von Behörden etc. haben längere und damit zumutbare Fristen, auch für eine juristische Beratung.

Wir stellen an dieser Stelle bewusst die Frage in den Raum, ob solch eine kurze Frist, die gerade an Wochenenden mit Feiertagen faktisch technisch und personell nicht zu erreichen ist, mit den aktuellen Gesetzen und auch dem Grundgesetz vereinbar ist.

Diese kurze Frist würde dem Betroffenen nicht einmal die Möglichkeit eines Rechtswegs eröffnen, denn selbst die Not-Gerichtsbarkeit mit Eilverfahren dürfte nicht derart schnell reagieren können.

Wir geben Ihnen persönlich bewusst und abschließend exemplarisch die Fragen mit: Wenn Sie für sich selbst eine Domain registrieren, z.B. „hans-mustermann-mdb.de“:

- Würden Sie selbst für eine „Verifikation“ persönlich zur Verfügung stehen?
- Würden Sie gerne Ihren Personalausweis vor eine Kamera halten?
- Würden Sie Ihre private Handy-Nummer in einer solchen Datenbank sehen wollen?
- **Würden Sie Ihre private Anschrift in einer solchen Datenbank sehen wollen?**

Denn: Die Identifizierbarkeit im aktuellen Entwurf legt nahe, dass dazu bei nicht-natürlichen Personen (also wie Sie als Abgeordnete*r) deren Privatanschrift hinterlegt werden muss – eine Geschäftsadresse wie das eigene Büro würde nicht ausreichen, denn die ist ja über den Personalausweis gar nicht verifizierbar.

Wir erwähnen an dieser Stelle bewusst auch, dass die aktuellen Forderungen und Teile des Gesetzesentwurfs dem Prinzip der Datensparsamkeit der EU-DSGVO entgegenstehen. Der Datenschutz wird dadurch in vielen Teilen unterlaufen bzw. unterwandert bzw. teilweise ad absurdum geführt.

Wir bitten an dieser Stelle darum,

1. die Bitte des Bundesrats mit Bezug auf a) abzulehnen
2. die §§ 49 und 50 des aktuellen Entwurfs zu überarbeiten und praxis-nah zu gestalten

Für Rückfragen, insbesondere eine persönliche Stellungnahme, stehe ich gerne zur Verfügung:

E-Mail manuel.schmitt@manitu.de

Mit freundlichen Grüßen

Manuel Schmitt