Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2024–2025

35 646 Regels voor het inzichtelijk maken van donaties ontvangen door maatschappelijke organisaties en tot het tegengaan van ondermijning door maatschappelijke organisaties, alsmede tot wijziging van het Burgerlijk Wetboek, de Handelsregisterwet 2007 en de Wet op de economische delicten in verband met het deponeren van de balans en de staat van baten en lasten door stichtingen (Wet transparantie en tegengaan ondermijning door maatschappelijke organisaties)

Nr. 9 **AMENDEMENT VAN HET LID SIX DIJKSTRA**

Ontvangen 10 december 2024

De ondergetekende stelt het volgende amendement voor:

Artikel 6 wordt als volgt gewijzigd:

1. In onderdeel a vervalt «en».

2. In onderdeel b wordt de punt aan het slot vervangen door «; en».

3. Er wordt een onderdeel toegevoegd, luidende:
c. de beveiliging van donatiegegevens.

Toelichting

De Wet transparantie en tegengaan ondermijning door maatschappelijke organisaties legt maatschappelijke organisaties de plicht op om de gegevens van donateurs zeven jaar te bewaren. Deze wettelijk bepaalde bewaartermijn, evenals de aanvullende regels over de aard en de wijze van de te verstrekken informatie, geeft organisaties naar opvatting van indiener tevens de verantwoordelijkheid om de confidentialiteit, integriteit en beschikbaarheid van de gegevens in kwestie te waarborgen, zodat donateurs ervanuit mogen gaan dat hun persoonlijke informatie voldoende beschermd is tegen datalekken. Indiener hoopt dat dit eraan bijdraagt dat de wet geen negatieve invloed zal hebben op de donatiebereidheid van mensen. Indiener beoogt mogelijk te maken dat middels een algemene maatregel van bestuur (AMvB) additionele regels kunnen worden gesteld over de basisbeveiligingsmaatregelen die maatschappelijke organisaties zouden moeten treffen om donatiegegevens te beveiligen. Hierbij denkt indiener specifiek aan het treffen van (digitale) beveiligingsmaatregelen waarbij al redelijkerwijs van organisaties

kst-35646-9
ISSN 0921 - 7371
's-Gravenhage 2024

verwacht zou mogen worden dat deze getroffen zijn, en die geen onnodige extra regeldruk op zouden moeten leveren. De Autoriteit Persoonsgegevens noemt specifiek de volgende basismaatregelen die organisaties zouden moeten treffen om zich te weren tegen het gros van hackaanvallen:[1]

1. Het inregelen en afdwingen van meerfactorauthenticatie (MFA);
2. Het opstellen van een goed wachtwoordbeleid;
3. Het tijdig uitvoeren van updates;
4. Het zorgen voor voldoende netwerksegmentatie.

Indiener ziet voor zich dat vergelijkbare basismaatregelen in de AMvB worden opgenomen. De voorgestelde wijziging van het betreffende wetsartikel is bewust algemeen en technologie-onafhankelijk opgesteld, zodat per algemene maatregel van bestuur nader ingevuld en aangevuld kan worden wat het basisniveau van beveiliging bij donatiegegevens zou moeten zijn, zonder dat dit een wetswijziging zou vereisen. Zo is het voorzienbaar dat op termijn nadere eisen gesteld worden aan het niveau van quantumveiligheid van systemen.

Six Dijkstra

[1] Autoriteit Persoonsgegevens, «Rapportage Ransomware» (22 oktober 2024), via https://www.autoriteitpersoonsgegevens.nl/documenten/rapportage-ransomware.