2 SEP 2026

AB2026026

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

> Retouradres Postbus 20011 2500 EA Den Haag

Gemeentelijk Belastingkantoor Twente
Ter attentie van de bestuurder van uw organisatie
Postbus 845
7550 AV Hengelo

**DG Digitalisering & Overheidsorganisatie**

Turfmarkt 147
2511 DP Den Haag
Postbus 20011
2500 EA Den Haag
www.rijksoverheid.nl

**Contact**

Cyberbeveiligingswet@minbzk.nl

Datum 26 augustus 2026
Betreft Cyberbeveiligingswet in werking 15 augustus 2026

**Onze referentie**
2026-0000436468

Geachte bestuurder,

Graag wil ik u erop attenderen dat de Cyberbeveiligingswet op 15 augustus 2026 in werking is getreden. De Cyberbeveiligingswet heeft mogelijk gevolgen voor uw organisatie. Deze is namelijk van toepassing op alle ministeries, provincies, gemeenten en op veel gemeenschappelijke regelingen en zelfstandige bestuursorganen[1]. Organisaties die onder de Cyberbeveiligingswet vallen, zijn verplicht hun digitale weerbaarheid te verhogen. Burgers en bedrijven moeten er immers op kunnen vertrouwen dat hun gegevens bij de overheid veilig zijn. In deze brief wordt u geïnformeerd over het doel van de Cyberbeveiligingswet, de verplichtingen die hieruit volgen en uw verantwoordelijkheden als bestuurder bij de naleving van deze verplichtingen.

**Doel van de Cyberbeveiligingswet**

De Cyberbeveiligingswet (Cbw), de nationale implementatie van de Europese NIS2-richtlijn, verplicht organisaties hun digitale weerbaarheid te verhogen. Het verhogen van digitale weerbaarheid is hard nodig. De afgelopen jaren wordt duidelijk hoe geopolitieke spanningen zich vertalen richting het digitale domein. Er is een grote verscheidenheid aan aanvallen door statelijke actoren, cybercriminelen en andere kwaadwillenden. Digitale dreigingen ondermijnen het vertrouwen in de overheid. Digitale veiligheid is geen luxe, maar een basisvoorwaarde voor een functionerende democratie. Aan ons de taak dit goed te beschermen.

**Verplichtingen**

Binnen de overheid geldt de Cbw voor de ministeries (inclusief dienstonderdelen en agentschappen), gemeenten, provincies, waterschappen en voor veel gemeenschappelijke regelingen en zelfstandige bestuursorganen. Voor gemeenschappelijke regelingen en zelfstandige bestuursorganen is dit afhankelijk van de organisatie (zie voor nadere uitleg hierover Bijlage I van deze brief).

Deze organisaties hebben vanuit de Cbw de volgende verplichtingen:

- Een registratieplicht om uw organisatie te registreren via het portaal van het Nationaal Cyber Security Centrum (NCSC).

[1] Is uw organisatie een gemeenschappelijke regeling of een zbo? Lees dan bijlage I van deze brief goed door.

- Een zorgplicht die uw organisatie verplicht om op basis van mogelijke risico's passende maatregelen te treffen voor het beveiligen van uw netwerk- en informatiesystemen en deze te controleren op effectiviteit. Daarbij is het nodig ook afhankelijkheden van leveranciers en ketenpartners mee te nemen.
- Een meldplicht om significante incidenten zo snel mogelijk, maar in elk geval binnen 24 uur te melden bij het Computer Security Incident Response Team (CSIRT) en de toezichthouder. In de praktijk gebeurt dit via het NCSC-portaal. Na een melding kan ondersteuning worden gekregen van het CSIRT bij het oplossen van het incident.
- Een trainingsverplichting voor de bestuurders van organisaties. Deze training heeft als doel dat u als bestuurder de risico's voor de cybersecurity van uw organisatie en beveiligingsmaatregelen beter kunt beoordelen en uw verantwoordelijkheid goed kunt invullen.

**Toezichthouder Cyberbeveiligingswet overheidsorganisaties**
Onderdeel van de Cyberbeveiligingswet is dat onafhankelijk toezicht gehouden wordt op de verplichtingen. Voor overheidsorganisaties – uitgezonderd de waterschappen – is dit de Rijksinspectie Digitale Infrastructuur (RDI). De RDI heeft verschillende instrumenten om de naleving van de wet en regels te bevorderen. Zo deelt RDI haar kennis over digitale weerbaarheid, kan de RDI handhaven op geconstateerde overtredingen of - als laatste pressiemiddel - een bestuurlijke boete of sanctie opleggen.

**Verantwoordelijkheden bestuurders overheidsorganisaties**
In de Cyberbeveiligingswet is bestuurlijke verantwoordelijkheid voor cybersecurity een belangrijk uitgangspunt. U bent u als bestuurder eindverantwoordelijk voor de integrale beveiliging van uw (digitale) organisatie. Concreet is de bestuurder – bent u – verantwoordelijk voor:

- Het maken van een risicoanalyse voor uw organisatie, inclusief uw toeleveringsketen.
- Het goedkeuren van maatregelen om deze risico's te mitigeren.
- Het volgen van een training binnen twee jaar na inwerkingtreding van de Cyberbeveiligingswet. Dit houdt ook in dat u uw kennis actueel moet houden want cyberbeveiliging is nooit 'af'. Op dit moment zijn het Rijk en de verschillende bestuurslagen bezig met het vormgeven van de gewenste inhoud voor deze training. De VNG heeft daarnaast al een syllabus gepubliceerd over de training voor bestuurders die ook voor andere bestuurslagen goed bruikbaar is[2].

Hoewel u als bestuurder eindverantwoordelijk bent, bestaan er natuurlijk verschillende experts binnen uw organisatie die bijdragen aan de invulling van Cbw-verplichtingen. Deze experts moeten u ondersteunen in uw verantwoordelijkheid als bestuurder. Aan u de taak om deze personen actief te betrekken. Denk bijvoorbeeld aan uw Chief Information Security Officer (CISO) die u vanuit een onafhankelijke positie advies over informatiebeveiliging kan geven.

[2] De VNG-syllabus Cyberbeveiligingswet is te raadplegen via VNG.nl

Goede samenwerking binnen uw eigen organisatie en met andere (overheids)organisaties is cruciaal om de overheid weerbaarder te maken. Daarnaast is het ter invulling van uw verantwoordelijkheid van belang om na te gaan of de governance, beschikbare capaciteit, deskundigheid en middelen binnen uw organisatie aansluiten op de verplichtingen van de Cyberbeveiligingswet.

**Bestaande aansprakelijkheid bestuurders overheidsorganisaties**
De Cyberbeveiligingswet bevat een bepaling over de aansprakelijkheid voor bestuurders wanneer verplichtingen van de richtlijn niet worden nagekomen. Deze bepaling is niet van toepassing voor overheidsinstanties. De Cyberbeveiligingswet brengt voor overheidsbestuurders geen nieuwe aansprakelijkheden met zich mee, buiten dat wat al bestond. Bestuurders kunnen nu al bij grove nalatigheid aansprakelijk worden gesteld. Dit betekent dat een bestuurder vervolgd (en veroordeeld) kan worden of een boete kan krijgen om de ontstane schade aan een ander te vergoeden. Dit verandert niet als gevolg van de Cbw.

**Bestuurders van overheidsorganisaties volgens de Cbw**
Per overheidsbestuurslaag bevat de Cyberbeveiligingswet een uitwerking van wat moet worden gezien als de bestuurders[3]:

| Bestuurslaag | Bestuurder |
|---|---|
| Ministeries | De minister |
| Zelfstandige bestuursorganen | Het zelfstandige bestuursorgaan zelf |
| Provincies | Gedeputeerde Staten |
| Gemeenten | Het college van B&W |
| Gemeenschappelijke regelingen | Het dagelijks bestuur van het openbaar lichaam, het bestuur van de bedrijfsvoeringsorganisatie of het gemeenschappelijk orgaan |

**Registratieplicht**
Organisaties die onder de Cyberbeveiligingswet vallen, moeten zich op 15 augustus 2026 hebben geregistreerd via MijnNCSC. Voor het vergemakkelijken van uw registratie voor de Cyberbeveiligingswet, is een koppeling gemaakt met het Register van Overheidsorganisaties. De gegevens van uw organisatie die al bekend zijn, worden ingeladen in het registratieportaal van het NCSC.

**Ondersteuning implementatie Cyberbeveiligingswet**
Op verschillende manieren worden overheidsorganisaties ondersteund bij de implementatie van de Cyberbeveiligingswet. Zo wordt via websites als www.digitaleoverheid.nl en www.bio-overheid.nl algemene, uitgebreide informatie over de verplichtingen van de Cyberbeveiligingswet gegeven en tools aangereikt die handig zijn voor uw organisatie. Voor de uitwerking en implementatie binnen uw eigen bestuurslaag kunnen aanvullende handreikingen en ondersteuning

[3] Cyberbeveiligingswet, art 24, lid 12

**DG Digitalisering & Overheidsorganisatie**
DGDOO-DS-Afdeling C

**Datum**

**Onze referentie**
2026-0000436468

beschikbaar zijn via de koepelorganisaties. Daarnaast is het mogelijk om vragen en suggesties in te sturen via: cyberbeveiligingswet@minbzk.nl.

Met de Cyberbeveiligingswet maken we Nederland samen digitaal veiliger. Cyberveiligheid is namelijk een continue zorg, het is nooit 'af'. Ik vertrouw erop dat wij als overheid ons intrinsiek verantwoordelijk voelen voor de digitale veiligheid van alle opgeslagen gegevens van burgers en organisaties, en dat wij ons tot het uiterste zullen inspannen om dat te garanderen.

Hoogachtend,

Eric van der Burg
Staatssecretaris van Binnenlandse
Zaken en Koninkrijksrelaties

**DG Digitalisering & Overheidsorganisatie**
DGDOO-DS-Afdeling C

**Datum**

**Onze referentie**
2026-0000436468

## Bijlage I voor gemeenschappelijke regelingen en zbo's

### Toetsen van overheidscriteria

Voor gemeenschappelijke regelingen en zelfstandige bestuursorganen (zbo's) geldt dat zij moeten voldoen aan de vier overheidscriteria uit de Cbw om onder deze wet te vallen[4]. Bent u een gemeenschappelijke regeling of een zbo? Dan moet u zo spoedig mogelijk verifiëren of de betreffende overheidscriteria op u van toepassing zijn. Uw bevinding moet u inclusief een motivatie toesturen naar cyberbeveiligingswet@minbzk.nl.

### Eerdere brief

Het ministerie van Binnenlandse Zaken en Koninkrijksrelaties heeft in december 2025 ook een brief gestuurd naar ca. 220 van de 440 gemeenschappelijke regelingen en 52 van de ca. 180 zbo's. Deze brief is gestuurd aan organisaties waarvan het ministerie de inschatting heeft gemaakt – op basis van openbare informatie - dat zij mogelijk aan de criteria voor overheidsorganisaties voldoen. Deze brief van december 2025 bevatte ook het verzoek om te verifiëren of uw overheidsorganisatie aan de criteria voldoet. Veel organisaties hebben hierop gereageerd, maar nog niet allemaal. Mocht u de verificatie al hebben gedaan en de uitkomst heeft doorgegeven aan BZK, dan hoeft u dit niet opnieuw te doen.

### Eigen verantwoordelijkheid

Het ministerie van Binnenlandse Zaken en Koninkrijksrelaties kan niet bepalen of een gemeenschappelijke regeling of zbo voldoet aan de overheidscriteria omdat zij onvoldoende inzicht heeft in de specifieke taken en kenmerken van deze organisaties. Bovendien benoemt de Cyberbeveiligingswet de eigen verantwoordelijkheid van organisaties die onder de wet vallen. Daarom is een verificatie door uw eigen organisatie noodzakelijk. Door deze verificatie bijtijds uit te voeren, voorkomt u dat u niet voldoet aan de verplichtingen uit de Cbw.

### Registratie verplicht

Alle overheidsorganisaties die onder de reikwijdte van de Cyberbeveiligingswet vallen, dienen vanuit de registratieplicht op 15 augustus 2026 geregistreerd te zijn via het meld- en registratieportaal van het NCSC. Het is uw eigen verantwoordelijkheid om uw organisatie te registreren.

[4] Deze vier overheidscriteria staan opgenomen in de Memorie van Toelichting op de Cyberbeveiligingswet onder 5.1.2 of zijn te vinden op www.digitaleoverheid.nl onder de pagina 'Voor welke overheidsorganisaties geldt de Cyberbeveiligingswet?'

PostNL
Por
Por
Pay

SERV-ZZ#X870X0X#00#0000#
3800GB 2532