Datum
26 juni 2024

Onderwerp
Reactie op de Cyberbeveiligingswet (Cbw).

Auteurs
mr. Wouter Scherpenisse
mr. dr. Sascha van Schendel

Afdeling
Erasmus School of Law;
De auteurs zijn werkzaam binnen het Erasmus Centre of Law and Digitalization

Bezoekadres
Erasmus School of Law
Burgemeester Oudlaan 50
Sanders building (L)

Postadres
Postbus 1738
3000 DR Rotterdam

E scherpenisse@law.eur.nl
E s.vanschendel@law.eur.nl
W www.eur.nl

Zoals het beleidskompasformulier van de Cyberbeveiligingswet (hierna: Cbw) aangeeft beoogt de NIS2-richtlijn 'een hoog gemeenschappelijk niveau van cyberbeveiliging in de Europese Unie te bereiken, teneinde de werking van de interne markt te verbeteren.' Dit doel zou moeten worden bereikt door verschillen op het gebied van cyberbeveiligingseisen tussen lidstaten weg te nemen. Met de implementatie van de Cbw beoogt de Nederlandse wetgever invulling te geven aan dat streven. Het is op zijn plaats om in eerste instantie een compliment te maken over de wijze waarop er invulling is gegeven aan het ingewikkelde implementatieproces, waarbij zoveel belangen in het oog gehouden moeten worden. Daarnaast zouden wij graag via dit schrijven onze gedachten over een aantal onderdelen van het huidige voorstel willen openbaren en suggesties voorstellen voor het navolgende wetgevingsproces.

We zullen nader ingaan op de thema's: reikwijdte; verantwoordelijkheid van bestuur (*governance*); vrijwillige meldingen (*coordinated vulnerability disclosure*; informatiedeling; haalbaarheid verplichtingen; en delegatieterminologie.

Reikwijdte

Ten aanzien van de reikwijdte van het wetsvoorstel hebben we een suggestie en verzoek om verheldering. Wat betreft de suggestie richten we ons op de status van onderwijsinstellingen. De Memorie van Toelichting (hierna: MvT) stelt op dit punt dat er momenteel een impactanalyse gaande is om een besluit te nemen over of (en zo ja, welke) onderwijsinstellingen als essentiële entiteit of belangrijke entiteit dienen te worden aangewezen. We richten ons voor dit schrijven specifiek op de universiteiten.

Alhoewel het handhavingsregime dat geldt voor belangrijke entiteiten wellicht meer past bij universiteiten, zijn wij van mening dat, gebruikmakend van artikel 11 Cbw, universiteiten in aanmerking komen om als essentiële[1] entiteiten te worden aangewezen. Dit standpunt leunt op drie argumenten. Ten eerste, zoals kort wordt benoemd op p. 15 van de MvT, zijn kennisinstellingen een bron van (gevoelige) informatie die interessant is voor digitale spionage en meer algemene malicieuze bedoelingen, wat bij uitstek geldt voor (technische) universiteiten waar veel onderzoek plaatsvindt. Onder dit laatste vallen ook situaties waarbij op grote schaal wordt geprobeerd toegang te verkrijgen tot e-mailadressen van universiteitsmedewerkers door middel van *phishing*. Aangezien universiteitsaccounts een bepaalde autoriteit en betrouwbaarheid uitstralen, kunnen deze accounts misbruikt worden om

[1] De keuze voor universiteiten als essentiële entiteit in plaats van belangrijke entiteit sluit naar onze mening aan bij de nationale vitaalbeoordeling in de ontwrichting en bedreiging van nationale veiligheid die kan volgen bij het (langdurig) offline halen of ernstig verstoren van digitale infrastructuur van universiteiten.

intern en extern navolgende *phishing*-acties vorm te geven. Universiteitssystemen hebben daarnaast een sterk genetwerkte structuur waarmee het eenvoudig kan zijn voor cybercriminelen om via één account toegang te verkrijgen tot gedeelde omgevingen.

Ten tweede moet de belangrijke maatschappelijke functie van het onderwijs niet worden onderschat, wat ook terloops wordt benoemd in de MvT. Uiteraard geldt deze belangrijke maatschappelijke functie voor alle onderwijsinstellingen, maar zeker voor universiteiten gezien de omvang van de instituten en de koppeling van het onderwijs aan impactvol onderzoek. Onder meer het cyberincident dat heeft plaatsgevonden bij de Universiteit Maastricht toont aan hoe kwetsbaar het onderwijs kan zijn, met het oog op de digitale infrastructuur van de instellingen. Dit geldt in verhoogde mate voor het onderwijs dat zich heeft ontwikkeld na de COVID-pandemie, waarbij meer is ingezet op online en hybride onderwijs.

Ten derde is er nog een component die niet expliciet wordt benoemd in de MvT, maar die wij wel van belang achten voor de beslissing omtrent de reikwijdte voor onderwijsinstellingen, namelijk: de uit de Cbw volgende verplichtingen betreffende cyberweerbaarheid en veiligheid (met name de *governance*). Een van de kerngedachten achter de Cbw is dat cyberbeveiliging net zo sterk is als de zwakste schakel binnen de keten. Deze '*weakest-link* benadering' is ook relevant voor onderwijsinstellingen. Niet alleen de technische beveiliging van de digitale systemen zelf dient op orde te zijn, maar ook dat de cyberweerbaarheidskennis van studenten en medewerkers moet adequaat zijn, wil je voldoende weerbaar zijn tegen cyberincidenten. Vaak ontstaan er risico's door menselijke fouten, bijvoorbeeld doordat iemand op een *phishing*-link klikt. Het is dan ook van belang dat studenten en medewerkers aan universiteiten de juiste kennis verkrijgen op dit gebied, welke met de studenten ook verspreid wordt over overheid en bedrijf. Deze handschoen van kennisvergaring dient in eerste instantie opgepakt te worden door het bestuur van de universiteiten, gezien hun voorbeeldfunctie, en met het oog op artikel 26 Cbw biedt deze wet daar een afdwingbare mogelijkheid voor. In de paragraaf over 'Verantwoordelijkheid van bestuur (*governance*)' zullen we uitgebreider stilstaan bij dit specifieke artikel. De toepasbaarheid van de Cbw voor universiteiten zou het besef over het belang van cyberweerbaarheidskennis een extra impuls kunnen geven.

Naast het bovengenoemde achten wij het van belang om de keuzes omtrent de reikwijdte ten aanzien van overheidsinstanties die activiteiten uitvoeren op het gebied van nationale veiligheid, openbare veiligheid, defensie of rechtshandhaving te verhelderen. Op grond van artikel 6 Cbw zijn deze actoren uitgesloten van de reikwijdte van de Cbw, wat het gevolg is van artikel 2 lid 7 van de NIS2-Richtlijn. Ook kan ingevolge artikel 25 Cbw voor een specifieke entiteit die activiteiten uitvoert op het gebied van nationale veiligheid, openbare veiligheid, defensie of rechtshandhaving of die uitsluitend diensten verleent aan de in artikel 6, eerste lid, bedoelde overheidsinstanties, met betrekking tot die activiteiten of diensten de bevoegde autoriteit bij regeling of besluit, in overeenstemming met de Minister, ontheffing worden verleend van de verplichtingen bedoeld in artikel 23. Tegelijkertijd zijn dit, met name de eerstgenoemde overheidsinstanties, wel degelijk cruciale actoren binnen het grotere plaatje van cyberbeveiliging binnen Nederland. Daarom is het belangrijk om een duidelijke uitleg en visie te presenteren over hoe deze actoren betrokken worden bij het cyberbeveiligingsvraagstuk en eventueel informatie kunnen delen met actoren die wel onder de Cbw vallen. Hierbij valt een vergelijking te trekken met het gegevensbeschermingsrecht, waar de Algemene Verordening Gegevensbescherming (hierna: AVG)[2] geldt als het

[2] Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming).

algemene kader voor de verwerking van persoonsgegevens en er daarnaast de EU-Politierichtlijn bestaat als een apart regime voor de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen.[3] Dit voorbeeld schetst dat het mogelijk is om een apart regime vorm te geven aan de hand van (met name) uitzonderingen op het gebied van transparantie en openbaarmaking van gegevens in het belang van onder andere de nationale veiligheid en bescherming van het strafrechtelijk onderzoek, terwijl daarnaast algemene regels en belangrijke principes kunnen bestaan die voor alle sectoren relevant zijn.

Verantwoordelijkheid van bestuur (*governance*)

Graag besteden we nog enige aandacht aan artikel 26 Cbw. Ingevolge dit artikel wordt de verantwoordelijkheid van bestuurders van essentiële en belangrijke entiteiten op het gebied van cyberbeveiliging vormgegeven. Uit het eerste lid volgt dat bestuurders de maatregelen uit artikel 23 Cbw dienen goed te keuren en toezien op de uitvoering van de maatregelen. Daarbij, zo vermeld het tweede lid van artikel 26 Cbw, is het wel nodig dat bestuurders daarvoor over de juiste kennis beschikken. Deze kennis zal in de vorm van (herhaaldelijke) trainingen overgebracht dienen te worden aan de bestuurders. De MvT stipt terecht het belang van dergelijke trainingen aan: *"Bestuursleden spelen een cruciale rol in het neerzetten van een sterke cyberweerbaarheidscultuur. [...] Vanuit die voorbeeldfunctie dragen ze cyberbewustheid uit, en moedigen werknemers binnen hun organisatie aan soortgelijke trainingen te volgen."*[4]

In het achtste lid van artikel 26 Cbw wordt bepaald dat 'de ambtelijke leiding' van een ministerie; provincie; gemeente; waterschap; of gemeenschappelijke regeling, wordt aangewezen als het bestuur. Als we ons richten op de ministeries, houdt deze aanwijzing in dat de bestuursraad - waar in elk geval de secretaris-generaal toe behoort – de beschreven verantwoordelijkheden uit artikel 26 Cbw toebedeeld krijgt.[5] Uit de MvT volgt dat het kabinet deze keuze het meest geschikt vond, omdat de ambtelijk leiding al verantwoordelijk is voor de uitvoering van de dagelijkse werkzaamheden.[6] Dit beoordelen wij als een logische afweging.

Aansluitend wordt genoemd dat de te volgen opleiding om kennis en vaardigheden op te doen met betrekking tot cyberbeveiliging, niet goed past bij politiek benoemde ambtsdragers, zoals bijvoorbeeld een Minister. Ook zou het sanctioneren van deze ambtsdragers niet passen bij de aard van hun benoeming.[7] Over dit laatste standpunt zijn weinig opmerkingen te maken. Toch zouden wij de wetgever graag ter overweging mee willen geven dat het (in verplichte vorm) opdoen van kennis over cyberveiligheid voor politiek benoemde ambtsdragers wellicht nog niet zo verkeerd is. Het feit dat besturen van essentiële en belangrijke entiteiten potentieel impactvolle besluiten dienen te nemen, is in een minstens zo ingrijpende mate van toepassing op bijvoorbeeld ministers. Denk daarbij aan het scenario dat besluiten gedurende een cyberincident onder tijdsdruk genomen dienen te worden in de Ministeriële Commissie Crisisbeheersing (MCCb).[8] Om ten slotte het

[3] Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad.
[4] Memorie van Toelichting, p. 23.
[5] We richten ons nu specifiek op ministers, maar soortgelijke argumenten kunnen (in mindere mate) ook voor andere politiek benoemde ambtsdragers worden gebruikt.
[6] Memorie van Toelichting, p. 24.
[7] Idem.
[8] NCTV, *Landelijk Crisisplan Digitaal,* december 2022, p. 27.

bovengenoemde citaat gedeeltelijk te gebruiken: *Ministers spelen een cruciale rol in het neerzetten van een sterke cyberweerbaarheidscultuur. [...] Vanuit die voorbeeldfunctie dragen ze cyberbewustheid uit, en moedigen de maatschappij aan soortgelijke trainingen te volgen."*

Vrijwillige meldingen (*coordinated vulnerability disclosure*)

Ook kijken we nog graag naar artikel 36 Cbw, betreffende de vrijwillige meldingen van kwetsbaarheden. Het eerste lid benoemt dat eenieder op vrijwillige basis een melding kan maken van een kwetsbaarheid bij de coördinator (CSIRTs) met het oog op een gecoördineerde bekendmaking van kwetsbaarheden. In de praktijk wordt veelal gesproken over *'coordinated vulnerability disclosure'* (hierna: CVD). Nederland heeft zich op dit terrein laten gelden als koploper en deze wettelijke verankering van dit onderdeel van CVD is een mooie stap in de richting van het bieden van zekerheid aan potentiële melders.

Uit onderzoek blijkt de 'cruciale rol' van vrijwillige beveiligingsonderzoekers en wordt er geconstateerd dat deze vrijwilligers, bijvoorbeeld verenigd in het DIVD, voorzien in een 'hiaat' door te scannen naar kwetsbare organisaties en deze organisaties te waarschuwen (bv. doelwitnotificatie).[9] Ook vanuit het NCSC en het OM wordt de positieve bijdrage van CVD-meldingen aan de digitale veiligheid onderschreven.[10] De MvT van de Cbw geeft aan dat onder de Cbw een 'coördinator' (mogelijk NCSC, Z-CERT, IBD e.d.) als tussenpersoon zal optreden tussen de melder en de fabrikant of aanbieder van mogelijk kwetsbare ICT-producten of -diensten.[11] Het wetsvoorstel biedt daarmee ruimte voor vrijwillige meldingen aan CSIRTs, maar maakt niet duidelijk welke ruimte er bestaat voor een ander belangrijk onderdeel van CVD: doelwitnotificatie door vrijwilligers. Nu ligt het, met het oog op NIS2, niet voor de hand om bepalingen in de Cbw op te nemen die zich richten op taakverdelingen in de verhouding melder-fabrikant. Desondanks biedt de Cbw ruimte om CVD-beleid een expliciet onderdeel te maken van de 'technische, operationele en organisatorische maatregelen' die de betreffende entiteiten moeten nemen.[12] Onder meer de verhoogde bekendheid met CVD op deze manier, zou kunnen bijdragen aan het vertrouwen dat organisaties hebben in de CVD-meldingen die zij mogelijk zullen ontvangen. In paragraaf 5.3.4. van de MvT zou daar bijvoorbeeld aandacht aan kunnen worden besteed.

Momenteel stoelt het CVD-beleid veelal op een Leidraad van het NCSC en de 'OM-beleidsbrief ethisch hacken', waarbij de belangrijkste grondslagen uit de jurisprudentie rondom ethisch hacken voortvloeien.[13] Sinds 2013 wordt het CVD-proces in Nederland actief gestimuleerd door het NCSC.[14] Gezien het belang van CVD achten wij het wenselijk dat de wetgever zich, nu de mogelijkheid zich voordoet, alsnog buigt over de vraag op welke wijze er een formele grondslag kan worden geboden aan dit vraagstuk. De jurisprudentie en de genoemde documenten bieden een duidelijk uitgangspunt voor organisaties die CVD-beleid implementeren.

---

[9] Onderzoeksraad voor Veiligheid, *Kwetsbaar door software. Lessen naar aanleiding van beveiligingslekken door software van Citrix,* december 2021, p. 72, 105.
[10] NCSC, *Coordinated Vulnerability Disclosure: de Leidraad*, oktober 2018; OM-beleidsbrief Coordinated Vulnerability Disclosure van 14 december 2020 (kenmerk PaG/B&S/18501).
[11] Memorie van Toelichting, p. 27-28.
[12] Vgl. Paragraaf 16.1.3.1. Baseline Informatiebeveiliging Overheid (https://bio-overheid.nl/category/producten?product=BIO).
[13] NCSC, *Coordinated Vulnerability Disclosure: de Leidraad*, oktober 2018; OM-beleidsbrief Coordinated Vulnerability Disclosure van 14 december 2020 (kenmerk PaG/B&S/18501); Rb. Oost-Brabant 15 februari 2013, ECLI:NL:RBOBR:2013:BZ1163; Rb. Den Haag 17 december 2014, ECLI:NL:RBDHA:2014:15611; Rb. Den Haag 30 augustus 2018, ECLI:NL:RBDHA:2018:10451.
[14] NCSC, *Coordinated Vulnerability Disclosure: de Leidraad*, oktober 2018, p. 3.

Informatiedeling

Voor een robuust cybersecuritybeleid is informatiedeling cruciaal. Het voorstel lijkt dit uitgangspunt ook te omarmen. Flexibiliteit in het delen van informatie kan echter vragen omtrent rechtszekerheid en/of transparantie oproepen. In paragraaf 5.6.5. van de MvT wordt aangegeven dat bepaalde organisaties, aan welke informatie verstrekt kon worden, onder de Wbni werden aangewezen bij ministeriële regeling (als OKTT of CSIRT).[15] Dit overzicht lijkt met het intrekken van de Wbni te verdwijnen, aangezien de Cbw 'onder omstandigheden' bepaalde organisaties aan kan wijzen als relevante partij.[16] Het betreft in dit geval specifiek organisaties die fungeren als schakelorganisaties, welke *ad hoc* worden aangemerkt als relevante partij, zo begrijpen wij. Aansluitend is er de mogelijkheid om sommige schakelorganisaties ook met een blik op de toekomst in een concreet geval aan te merken als relevant, waarbij bepalend is of 'de achterban van aanbieders bestaat uit essentiële entiteiten, belangrijke entiteiten dan wel relevante partijen'.[17]

Ten eerste vragen we ons af of er, in het kader van transparantie, een soortgelijk inzicht wordt gegeven als onder de Wbni, in de aanmerking van dergelijke relevante partijen. Mede aangezien deze organisaties mogelijk vertrouwelijke gegevens kunnen ontvangen, ingevolge artikel 65 lid 2 Cbw. Ten tweede bestaat er onzerzijds wat onduidelijkheid over de aanwijzingen van relevante partijen met het oog op de toekomst in een concreet geval (zie paragraaf 5.6.5. van de MvT). Worden bepaalde organisaties voor langere duur aangemerkt als 'relevant'; worden er concrete gevallen gegeven waarbij deze partijen aan te merken zijn als relevant; of blijft het bij een *ad hoc* aanmerking?

Daarnaast wordt er in paragraaf 5.6.4 van de MvT ook stilgestaan bij de categorie relevante partijen. Hier betreft het echter niet specifiek schakelorganisaties. De relevantie van deze organisaties wordt, zo begrijpen wij, in beginsel *ad hoc* vastgesteld op basis van de relevantie van de informatie van een CSIRT voor de cyberweerbaarheid van de partijen zelf of hun achterban. Wat betreft de schakelorganisaties kan men zich op dit moment een redelijke (maar geen precieze) voorstelling maken van de organisaties die als relevant kunnen worden aangemerkt, bijvoorbeeld met een blik op het Landelijk Dekkend Stelsel. De reikwijdte van relevante partijen uit paragraaf 5.6.4. is echter lastiger in te schatten. Het zou goed zijn als daaromtrent meer duidelijkheid wordt gegeven, bijvoorbeeld in de vorm van algemene criteria. Ook bij deze categorie relevante partijen, waarop artikel 65 lid 2 Cbw van toepassing is, vragen we ons af op welke manier er met het oog op transparantie, inzicht wordt gegeven in de uiteindelijk aangemerkte partijen.

Hierbij merken we graag op dat we het belang van het delen van (vertrouwelijke) informatie wel degelijk onderschrijven. Een praktisch probleem uit zich bijvoorbeeld in de dubbele meldingen ('herontdekkingen') omtrent kwetsbaarheden.[18] Het makkelijker kunnen delen van bepaalde informatie met organisaties, van bijvoorbeeld (vrijwillige) beveiligingsonderzoekers, die gelijktijdig werk verrichten in de bestrijding van eenzelfde cyber-incident zou in dat kader zeer waardevol kunnen zijn. Het delen van dergelijke informatie moet echter niet te lichtvaardig worden gedaan. Duidelijke waarborgen, bijvoorbeeld in de aanmerking van organisaties of het toezicht daarop, lijken op hun plaats.

Haalbaarheid verplichtingen

Een belangrijk aspect van dit soort van wetgevingsprocessen betreft de haalbaarheid van de voorgestelde verplichtingen. De praktische implicaties van de Cbw zijn wat dat betreft erg relevant. Sectie 8 van de MvT gaat hierop

[15] Regeling aanwijzing schakelorganisaties cybersecurity (*Stcrt.* 2022, 32041).
[16] Zie hiervoor artikel 17 lid 2 onderdeel b Cbw.
[17] Memorie van Toelichting, p. 29.
[18] T. Herr, B. Schneier & C. Morris, *Taking Stock: Estimating Vulnerability Rediscovery* (Belfer Cyber Security Project White Paper Series), juli 2017 (herzien: oktober 2017).

in aan de hand van regeldruk en kosten, waar wellicht een optimistische toon wordt gekozen. Er wordt erkend dat de Cbw van toepassing zal zijn op aanzienlijk meer entiteiten dan de Wbni, maar tegelijkertijd wordt ervan uitgegaan dat veel entiteiten zonder verplichtingen uit wetgeving al beveiligingsmaatregelen treffen. Daarnaast wordt geschat dat de toename van ICT-beveiligingskosten voor nieuwe entiteiten maximaal 22% bedraagt. Ook worden er schattingen gepresenteerd in sectie 8.1.3 (meldplicht) en 8.1.4. (Registratieplicht) van de MvT. Alhoewel dergelijke inzichten heel waardevol zijn, blijft het onduidelijk hoe deze precies tot stand zijn gekomen, waarmee de mogelijkheid lijkt te bestaan dat de schattingen achteraf te optimistisch zijn geweest. Het ligt voor de hand dat sommige entiteiten waarschijnlijk meer tijd nodig hebben dan entiteiten die al voorzien hebben in bestaande cyberbeveiligingsstructuren, kennis, en maatregelen. Daarnaast blijkt het in de praktijk zelfs voor entiteiten waarvan verwacht wordt dat zij adequate cyberbeveiligingsstructuren hebben, toch een grote opgave om te zorgen voor voldoende bescherming voor het hele systeem (inclusief de zwakste schakels). Een recent voorbeeld hiervan is de cyberbeveiliging binnen lokale overheden waarbij niet alle websites blijken te voldoen aan beveiligingsstandaarden.[19] Daarnaast is het onduidelijk of de benodigde experts die de veranderingen onder de Cbw vorm moeten geven beschikbaar zijn.

Het is belangrijk om hiermee rekening te houden bij het bepalen van de termijn waarop de verplichtingen uit de Cbw worden gehandhaafd en om regelmatig in contact met stakeholders te treden om te evalueren of deze schattingen inderdaad correct en haalbaar zijn.[20] Bij een tekort aan personen met de relevante (technische) kennis ontstaat het risico op een *'tick the box exercise'* door in documentatie en verantwoording vooral aandacht te besteden aan de wettelijke verplichtingen, in plaats van het daadwerkelijk verbeteren van de cyberbeveiliging. Op dit punt kan ook lering worden getrokken uit de ervaringen met de AVG. Hier gelden ook verschillende meldplichten en in de praktijk, gezien de hoge boetes, legt dat soms een te grote nadruk op de (administratieve) naleving van de letter der wet, zowel binnen de toezichthouder als binnen organisaties zelf.[21]

Delegatieterminologie

Een laatste opmerking betreft het gebruik van juridische terminologie. Zo spreekt de MvT over verschillende 'delegatiegrondslagen' waar expliciet ruimte voor subdelegatie wordt gezocht. Het is aan te raden om ten aanzien van bepalingen waarin de terminologie 'bij of krachtens algemene maatregel van bestuur' wordt gehanteerd, duidelijk de mogelijkheid tot subdelegatie te benoemen.[22] Denk bij dit laatste bijvoorbeeld aan de voorlaatste alinea van pagina 22 van de MvT.[23]

Pagina 77 van de MvT schetst waarom het van belang is om zorgvuldig te zijn met delegatieterminologie. Zo wordt in de MvT subdelegatie in artikel 37 Cbw

[19] Zie 'Duizenden 'vergeten' gemeentelijke websites in ontluisterende staat', Hartholt 29 februari 2024, via: https://www.binnenlandsbestuur.nl/digitaal/duizenden-websites-gemeenten-slechte-staat.
[20] De minister van Justitie en Veiligheid spreekt over het tweede of derde kwartaal van 2025 (*Aanhangsel Handelingen II* 2023/24, nr. 1866, p. 2, 4).
[21] Voorbeelden hiervan zijn concreet terug te vinden in onderzoek uitgevoerd voor het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC) in: Winter, H., Drouen, T., Eck, M. V., Geertsema, B., Cazemier, J., & Ridderbos-Hovingh, C. (2022) Bescherming gegeven? Evaluatie UAVG, meldplicht datalekken en de boetebevoegdheid. Pro Facto (zie de conclusies en aanbevelingen); Zie ook, over de discrepantie tussen naleving en daadwerkelijke bescherming, studies over de AVG in Nederland die bijvoorbeeld focussen op bescherming van de betrokkenen en percepties over de wetgeving: Strycharz, Ausloos, & Helberger (2020). Data protection or data frustration? individual perceptions and attitudes towards the gdpr. European Data Protection Law Review (EDPL), 6(3), 407-421.
[22] Zie aanwijzing 2.24 en 2.26 van de Aanwijzingen voor de regelgeving.
[23] Zie ook pagina 11, 24, 71, 77 en 79.

uitgesloten (‘bij amvb’), terwijl artikel 37 zelf wel degelijk voorziet in de mogelijkheid tot subdelegatie (‘Bij of krachtens algemene maatregel van bestuur’).