Position Paper "Nazorgplicht bij datalekken"

Oproep Cyberveilig Nederland

De brancheorganisatie voor cybersecurity dienstverleners (CVNL) pleit voor slachtoffergericht en proportionele nazorgplicht bij datalekken, die voortbouwt op bestaande regels. Reden hiervoor is dat de problemen voor secundaire slachtoffers[1] immers pas beginnen ná de melding van een datalek, terwijl de wettelijke verplichtingen voor organisaties daar grotendeels eindigen. De bestaande regels richten zich vooral op preventie en melding; voor de nazorg ná een datalek – concrete informatie en een vangnet – ontbreekt nog een duidelijke norm. Een nazorgplicht vult dat gat, zonder een zwaar nieuw regime toe te voegen. Datalekken zoals bij Clinical Diagnostics en Odido laten zien dat secundaire slachtoffers op zichzelf zijn aangewezen en onvoldoende ondersteuning ontvangen. De actualiteit maakt dit urgent: met de Digitale Omnibus worden de Europese regels voor incidentmelding en informatievoorziening nu herzien, wat het moment biedt om de nazorg aan slachtoffers structureel te verankeren.

> Cyberveilig Nederland roept op om het bestaande toezicht te versterken, daarbinnen de informatiepositie van slachtoffers te beschermen, een vangnet voor slachtoffers daarbuiten te organiseren, zorgvuldig en transparant om te gaan met losgeldbetalingen, en het stelsel lerend te maken.

Vooropgesteld, de getroffen organisatie is in de eerste plaats zelf slachtoffer en mag niet als dader worden behandeld. Een nazorgplicht moet dus proportioneel zijn: gericht op wat slachtoffers écht nodig hebben, maar uitvoerbaar voor organisaties van verschillende omvang. Tevens moet een nazorgplicht aansluiten bij de Algemene verordening gegevensbescherming (AVG) en gelden voor álle organisaties die persoonsgegevens verwerken[2].

Concreet vragen wij wetgever, beleidsmakers en toezichthouders om het volgende.

1. **Versterk het bestaande toezicht.**
   Het kernprobleem is niet een gebrek aan regels, maar gebrekkige naleving en te weinig capaciteit voor handhaving en toezicht. Zo constateert de Autoriteit Persoonsgegevens (AP) in haar Position Paper Cyberveiligheid en Informatiebeveiliging[3] (19 mei 2026) dat organisaties basismaatregelen zoals snelle en adequate informatievoorziening aan slachtoffers onvoldoende naleven. In 2025 ontving de AP ruim 44.000 datalekmeldingen, maar startte zij slechts 25 onderzoeken bij circa 5.300 cybergerelateerde datalekken (AP, Jaarverslag 2025); tegelijk daalt haar budget van €55,8 miljoen (2025) naar €53,5 miljoen (2026) (Kamerstukken II, Begroting JenV).

[1] https://cyberveilignederland.nl/upload/userfiles/images/news/Melissa_Best%20practices%20secundair%20slachtofferschap_v2_2_digitaal.pdf
[2] De Cyberbeveiligingswet (de Nederlandse uitwerking van NIS2) ziet alleen op essentiële en belangrijke entiteiten en op 'significante incidenten', terwijl een datalek van persoonsgegevens onder de AVG valt. Juist het gros van de consument-rakende datalekken – webshops, kleinere dienstverleners, het MKB – valt buiten de Cbw.
[3] Autoriteit Persoonsgegevens, Position paper cyberveiligheid en informatiebeveiliging (19 mei 2026), opgesteld voor het rondetafelgesprek van de Tweede Kamercommissie Digitale Zaken.

Oproep: Investeer in risicogestuurd toezicht door AP en in andere toezichthouders zoals de Rijksdienst Digitale Infrastructuur (RDI) en Inspectie Leefomgeving en Transport (IL&T). Dit toezicht moet zowel preventief zijn als na een incident. Op deze manier wordt toegezien dat bestaande verplichtingen daadwerkelijk worden nageleefd én tekortschietende nazorg achteraf wordt gehandhaafd.

2. **Bescherm de informatiepositie van (secundaire) slachtoffers**
   Slachtoffers worden na een datalek vaak te laat en te algemeen geïnformeerd. Dat geldt bij uitstek voor secundaire slachtoffers, deze informatie is vaak te beperkt om zichzelf effectief te kunnen beschermen tegen bijvoorbeeld fraude en identiteitsmisbruik. De AVG verplicht weliswaar tot het informeren van betrokkenen bij een hoog risico (art. 34 AVG), maar stelt weinig eisen aan de concreetheid daarvan. Tegelijk verhoogt de Digitale Omnibus de melddrempel – melden hoeft straks alleen nog bij datalekken met een waarschijnlijk hoog risico[4] – en verlengt de termijn naar 96 uur; De Nederlandse regering steunt vereenvoudiging, maar uit zelf grote zorgen over de gevolgen voor de bescherming van betrokkenen[5]. Om de ernst van een datalek – en daarmee de benodigde informatie – objectief te bepalen, biedt de ENISA-methodiek een bruikbare leidraad[6].

   Oproep: Veranker dat slachtofferinformatie begrijpelijk, concreet en risicogestuurd blijft. Gebruik daarvoor de ENISA Data Breach Severity Methodology[7] als leidraad.

3. **Organiseer een vangnet voor slachtoffers.**
   Datalekken kunnen voor getroffenen tot langdurige schade leiden en secundaire slachtoffers staan daarbij nu grotendeels alleen. Zij weten vaak niet waar ze terechtkunnen om zich te beschermen, hulp te krijgen of aangifte te doen. Een herkenbaar vangnet dat hen opvangt en de drempel tot aangifte verlaagt, is daarom essentieel – en levert het stelsel bovendien beter zicht op daders en werkwijzen op.

   Oproep: richt een herkenbaar vangnet in dat secundaire slachtoffers actief ondersteunt – met de Fraudehelpdesk en Slachtofferhulp als loket met mandaat en structurele middelen – en hen helpt zichzelf te beschermen en laagdrempelig aangifte te doen. Maak aangifte voor primaire en secundaire slachtoffers de norm en stimuleer een vrijwillige NCSC-melding voor primaire slachtoffers bij incidenten onder de meldplichtdrempel van de Cyberbeveiligingswet (Cbw) die wél persoonsgegevens raken.

---

[4] 'Hoog risico' (art. 34 AVG) betekent dat een datalek waarschijnlijk ernstige gevolgen heeft voor betrokkenen, zoals fraude of financiële schade. De Digitale Omnibus (COM(2025) 837) trekt de meldplicht aan de toezichthouder op naar deze zwaardere drempel, waar nu nog geldt: melden tenzij een risico onwaarschijnlijk is.
[5] BNC-fiche Omnibus AI en Omnibus Digitaal, kabinetsstandpunt, Tweede Kamer, Kamerstuk 22112 (12 december 2025).
[6] ENISA, Recommendations for a methodology of the assessment of severity of personal data breaches, Working Document v1.0 (december 2013).
[7] https://www.enisa.europa.eu/sites/default/files/publications/Data%20breach%20severity%20methodology_1.0.pdf

4. **Losgeld: niet betalen, tenzij – en altijd transparant**
   CVNL staat achter het overheidsstandpunt[8]: niet betalen. Toch kunnen er uitzonderlijke situaties bestaan, – zoals risico's voor de continuïteit van vitale processen of voor mensenlevens – die maken dat organisaties na grondige afweging toch besluiten te betalen.

   Oproep: Introduceer een meld- en verantwoordingsplicht bij de toezichthouder – AP - wanneer toch wordt betaald. Gebruik deze meldgegevens vervolgens om beter zicht te krijgen op losgeldbetalingen, aansluitend op de gestandaardiseerde EU-incidentrapportage die de Digitale Omnibus voorziet (één Europees meldpunt bij ENISA).

5. **Maak het stelsel lerend**
   Toezicht op datalekken is nu versnipperd over de AP (AVG) en de Cbw-toezichthouders – en bij het NCSC in geval van een vrijwillige melding onder de Cbw. Er is weinig zicht op wat in de praktijk wel en niet werkt qua (genomen) maatregelen. Onderzoekers aan de universiteiten en hogescholen kunnen hierbij helpen. Het is dus van belang dat er een uitwisseling komt tussen deze overheidsinstanties en wetenschap om zo zicht en inzicht te hebben op de (werking van) maatregelen in relatie tot een datalek. De Digitale Omnibus zet met een gestandaardiseerd EU-meldformulier een eerste stap richting uniforme data; het kabinet geeft daarbij de voorkeur aan het versterken van bestaande nationale meldstructuren boven een centraal Europees platform.

   Oproep: Institutionaliseer informatie-uitwisseling tussen AVG- en Cbw-toezicht en het NCSC vanuit de CSIRT taak. Geef onderzoekers toegang tot deze data over effectiviteit en impact en draag zorg dat deze opgedane informatie, trends en kennis beschikbaar gesteld wordt aan organisaties die tot taak hebben om te informeren over maatregelen of handelingsperspectief.

[8] NCSC, 'Wat te doen bij een ransomware-aanval' (advies: betaal geen losgeld, doe aangifte); kabinetsstandpunt, beantwoording Kamervragen, Aanhangsel Handelingen 2021–2022, nr. 225.

Achtergrond

Datalekken zijn geen incidenten meer, maar een structureel maatschappelijk probleem

Niemand wil ermee te maken krijgen: een cyberincident waarbij persoonsgegevens worden gestolen. Toch is dit inmiddels de regel, niet de uitzondering. Bij ransomware aanvallen is steeds vaker sprake van data-exfiltratie,[9] waarbij persoonlijke gegevens van klanten, patiënten of medewerkers worden buitgemaakt. Clinical Diagnostics, de gemeente Epe, Rituals, Basic Fit, Chipsoft en Odido zijn enkele recente voorbeelden die het nieuws hebben gehaald.

De schade stopt niet op het moment dat systemen zijn hersteld. Voor getroffen burgers - de 'secundaire' slachtoffers[10] - begint die dan pas. Gestolen NAW-gegevens, telefoonnummers, kopieën van identiteitsbewijzen, gezondheids- en salarisgegevens zijn handelswaar voor criminelen en worden ingezet voor identiteitsfraude, WhatsApp-fraude, phishing en andere vormen van misbruik. Elk datalek voedt zo nieuwe incidenten, die op hun beurt weer nieuwe datalekken veroorzaken. Wie de keten wil doorbreken, moet de nazorg na een incident net zo serieus nemen als de preventie ervóór. Voor een deel van de getroffenen leiden dergelijke incidenten bovendien tot persoonlijk lijden, gevoelens van onveiligheid en langdurige stress.[11]

Daarbij past één belangrijke kanttekening. De getroffen organisatie is in de eerste plaats zelf slachtoffer. In de beeldvorming – mede door media-aandacht – wordt zij echter al snel als dader neergezet, terwijl het in veel gevallen gaat om een combinatie van een systeemfout, naïviteit en pech bij organisaties die hun beveiliging juist grotendeels op orde hadden. De nazorgplicht moet daarom verplichtingen aan organisaties koppelen zonder hen onterecht te criminaliseren. Daarbij past nadrukkelijk een proportionaliteitstoets naar omvang en draagkracht. Een kleine onderneming die is gehackt, mogelijk losgeld of een boete betaalt én vervolgens fors moet investeren in nazorg en eventuele vergoedingen, kan daaraan onderdoor gaan. Verplichtingen uit deze paper moeten dan ook schaalbaar zijn, en voor partijen die niet bij een CSIRT terechtkunnen zou ondersteuning vanuit de overheid het sluitstuk moeten vormen.

---

[9] Vanuit project Melissa is hier een whitepaper over geschreven: https://cyberveilignederland.nl/upload/userfiles/files/VCNL_Whitepaper_Exfiltratie_v3_0_Web.pdf

[10] Vanuit project Melissa is hier een handreiking over geschreven: https://cyberveilignederland.nl/actueel/persbericht-samenwerkingsverband-melissa-publiceert-best-practices-secundair-slachtofferschap

[11] Cross, C., & Holt, T. J. (2025). Beyond fraud and identity theft: Assessing the impact of data breaches on individual victims. Journal of Crime and Justice. Advance online publication.