Position Paper "Duty of Aftercare in Data Breaches"

Call to Action – Cyberveilig Nederland

The association for cybersecurity service providers (CVNL) advocates a victim-centred and proportionate duty of aftercare in data breaches that builds on existing rules. The reason is that the problems for secondary victims[1] only begin after a data breach has been reported, whereas organisations' legal obligations largely end there. The existing rules focus mainly on prevention and notification; for aftercare following a breach – concrete information and a safety net – a clear standard is still lacking. A duty of aftercare fills that gap without adding a heavy new regime. Breaches such as those at Clinical Diagnostics and Odido show that secondary victims are left to depend on themselves and receive insufficient support. Current developments make this urgent: with the Digital Omnibus, the European rules on incident notification and information provision are now being revised, which offers the moment to safeguard aftercare for victims structurally.

> *Cyberveilig Nederland calls for strengthening existing oversight, protecting victims' information position within that oversight, organising a safety net for victims beyond it, handling ransom payments carefully and transparently, and making the system capable of learning.*

First and foremost, the affected organisation is itself a victim and must not be treated as a perpetrator. A duty of aftercare must therefore be proportionate: focused on what victims genuinely need, yet workable for organisations of varying size. Such a duty must also align with the General Data Protection Regulation (GDPR) and apply to all organisations that process personal data[2].

Concretely, we ask legislators, policymakers and regulators for the following.

1. **Strengthen existing oversight.**
   The core problem is not a lack of rules, but poor compliance and too little capacity for enforcement and oversight. The Dutch Data Protection Authority (AP), for example, notes in its *Position Paper on Cybersecurity and Information Security*[3] (19 May 2026) that organisations inadequately implement basic measures such as swift and adequate information provision to victims. In 2025 the AP received over 44,000 data breach notifications but opened only 25 investigations into some 5,300 cyber-related breaches (AP, Annual Report 2025); at the same time its budget is falling from €55.8 million (2025) to €53.5 million (2026) (Parliamentary Papers II, Ministry of Justice and Security budget).

[1] A practical guide on this was written as part of the Melissa project: https://cyberveilignederland.nl/upload/userfiles/images/news/Melissa_Best%20practices%20secundair%20slachtofferschap_v2_2_digitaal.pdf

[2] The Cybersecurity Act (the Dutch implementation of NIS2) covers only essential and important entities and 'significant incidents', whereas a breach of personal data falls under the GDPR. It is precisely the bulk of consumer-facing data breaches – web shops, smaller service providers, SMEs – that fall outside the Cbw.

[3] Dutch Data Protection Authority, Position Paper on Cybersecurity and Information Security (19 May 2026), prepared for the round-table discussion of the House of Representatives' Digital Affairs Committee.

Call: Invest in risk-based oversight by the AP and by other regulators such as the Dutch Authority for Digital Infrastructure (RDI) and the Human Environment and Transport Inspectorate (ILT). This oversight must be both preventive and post-incident. In this way it is ensured that existing obligations are actually complied with and that inadequate aftercare is enforced after the fact.

2. **Protect the information position of (secondary) victims**

   After a data breach, victims are often informed too late and too generally. This is especially true for secondary victims: the information provided is often too limited for them to protect themselves effectively against, for example, fraud and identity misuse. While the GDPR requires data subjects to be informed in the event of a high risk (Art. 34 GDPR), it sets few requirements as to how concrete that information must be. At the same time, the Digital Omnibus is raising the notification threshold – notification will soon only be required for breaches involving a likely high risk[4] – and is extending the deadline to 96 hours; the Dutch government supports simplification but has itself expressed serious concerns about the consequences for the protection of data subjects[5]. To determine the severity of a breach objectively – and thus the information required – the ENISA methodology offers a useful guide[6].

   Call: Ensure that information for victims remains comprehensible, concrete and risk-based. Use the ENISA Data Breach Severity Methodology[7] as a guide.

3. **Organise a safety net for victims.**

   Data breaches can cause lasting harm to those affected, and secondary victims are now largely left on their own. They often do not know where to turn to protect themselves, obtain help or file a police report. A recognisable safety net that supports them and lowers the threshold to reporting is therefore essential – and, moreover, gives the system better insight into perpetrators and their methods.

   Call: Establish a recognisable safety net that actively supports secondary victims – with the Fraud Help Desk (Fraudehelpdesk) and Victim Support Netherlands (Slachtofferhulp) as the point of contact, with a mandate and structural funding – and that helps them protect themselves and file a police report with a low threshold. Make reporting the norm for both primary and secondary victims, and encourage a voluntary NCSC notification for primary victims in incidents below the mandatory-notification threshold of the Dutch implementation of the NIS2 directive - Cyberbeveiligingswet (Cbw) that do nevertheless involve personal data.

---

[4] 'High risk' (Art. 34 GDPR) means that a data breach is likely to have serious consequences for data subjects, such as fraud or financial harm. The Digital Omnibus (COM(2025) 837) raises the notification obligation to the regulator to this higher threshold, whereas the rule currently is: notify unless a risk is unlikely.

[5] BNC-fiche on the AI Omnibus and Digital Omnibus (a Dutch government assessment of an EU proposal), government position, House of Representatives, Parliamentary Paper 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. **Ransom: do not pay, unless – and always be transparent**
   CVNL supports the government's position[8]: do not pay. Nonetheless, exceptional situations may arise – such as risks to the continuity of vital processes or to human lives – that lead organisations, after careful consideration, to decide to pay after all.

   Call: Introduce a notification and accountability obligation to the regulator – the AP – when payment is nevertheless made. Then use this notification data to gain better insight into ransom payments, in line with the standardised EU incident reporting that the Digital Omnibus provides for (a single European reporting point at ENISA).

5. **Make the system capable of learning**
   Oversight of data breaches is currently fragmented across the AP (GDPR) and the Cbw regulators – and the NCSC in the case of a voluntary notification under the Cbw. There is little insight into what does and does not work in practice in terms of the measures taken. Researchers at universities and universities of applied sciences can help here. It is therefore important that an exchange is established between these government bodies and academia, in order to gain insight and understanding into the (effectiveness of) measures in relation to a data breach. With a standardised EU notification form, the Digital Omnibus takes a first step towards uniform data; the government, however, prefers strengthening existing national reporting structures over a central European platform.

   Call: Institutionalise the exchange of information between GDPR and Cbw oversight and the NCSC in its CSIRT capacity. Give researchers access to this data on effectiveness and impact, and ensure that the resulting information, trends and knowledge are made available to organisations tasked with providing information on measures or courses of action.

[8] NCSC, 'What to do in a ransomware attack' (advice: do not pay ransom, file a police report); government position, answers to parliamentary questions, Appendix to the Proceedings 2021–2022, no. 225.

Background

Data breaches are no longer incidents but a structural societal problem

No one wants to face it: a cyber incident in which personal data are stolen. Yet this has become the rule rather than the exception. In ransomware attacks, data exfiltration is increasingly common,[9] whereby personal data of customers, patients or employees are captured. Clinical Diagnostics, the municipality of Epe, Rituals, Basic Fit, Chipsoft and Odido are a few recent examples that have made the news.

The harm does not stop the moment systems are restored. For affected citizens – the 'secondary' victims[10] – that is when it only begins. Stolen name and address details, telephone numbers, copies of identity documents, health and salary data are commodities for criminals and are used for identity fraud, WhatsApp fraud, phishing and other forms of misuse. Every data breach thus feeds new incidents, which in turn cause new breaches. Anyone seeking to break the chain must take aftercare following an incident as seriously as prevention beforehand. For some of those affected, such incidents moreover lead to personal suffering, feelings of insecurity and prolonged stress.[11]

One important caveat applies here. The affected organisation is first and foremost a victim itself. In public perception – partly owing to media attention – it is nonetheless quickly cast as the culprit, whereas in many cases this involves a combination of a system error, naivety and bad luck at organisations that in fact largely had their security in order. The duty of aftercare must therefore attach obligations to organisations without wrongly criminalising them. This calls emphatically for a proportionality test based on size and financial capacity. A small business that has been hacked, may pay a ransom or a fine, and must then invest heavily in aftercare and any compensation, could be pushed under by it. Obligations arising from this paper must therefore be scalable, and for parties that cannot turn to a CSIRT, support from the government should form the final safeguard.

[9] A white paper on this was written as part of the Melissa project: https://cyberveilignederland.nl/upload/userfiles/files/VCNL_Whitepaper_Exfiltratie_v3_0_Web.pdf

[10] A practical guide on this was written as part of the Melissa project: 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.