PROCEDURE

Meldprocedure en meldingenlogboek

Twee wetten kennen een meldplicht met een harde klok. De Cyberbeveiligingswet vraagt binnen 24 uur een vroegtijdige waarschuwing bij een ernstig incident; de AVG geeft 72 uur voor het melden van een datalek. Dit document zet de termijnen naast elkaar, legt vast wie wat doet en geeft een logboekformaat waarmee u de werking van het proces aantoont.

De twee meldplichten naast elkaar

	CYBERBEVEILIGINGSWET — ERNSTIG INCIDENT	AVG — DATALEK PERSOONSGEGEVENS
Wanneer melden	Bij een significant incident: ernstige verstoring van de dienst of aanzienlijke schade, ook als die dreigt	Bij een inbreuk op persoonsgegevens, tenzij een risico voor betrokkenen onwaarschijnlijk is
Eerste melding	Vroegtijdige waarschuwing binnen 24 uur	Melding bij de Autoriteit Persoonsgegevens binnen 72 uur
Vervolg	Volledige melding binnen 72 uur, eindverslag binnen een maand	Betrokkenen informeren bij hoog risico, zonder onnodige vertraging
Bij wie	Het NCSC als CSIRT en de toezichthouder van uw sector	De Autoriteit Persoonsgegevens, via het meldloket
Altijd registreren	Elk incident in het logboek, ook onder de meldgrens	Elk datalek in het interne register, ook zonder meldplicht

Wie doet wat

Vul namen en bereikbaarheid in en hang de tabel niet alleen in een beleidsstuk, maar ook naast het incidentproces.

STAP	NAAM EN ROL	BEREIKBAAR VIA
1. Incident vaststellen en ernst bepalen		
2. Besluit tot melden nemen		
3. Melden bij NCSC, toezichthouder of AP		
4. Betrokkenen en klanten informeren		
5. Registreren en evalueren		

Het meldingenlogboek

Eén regel per incident of datalek, ook wanneer melden niet verplicht was. De eerste regel is een ingevuld voorbeeld.

DATUM, TIJD	INCIDENT	ERNST	GEMELD BIJ	AFGEROND	GELEERD
3 nov, 09.40	Phishingmail geopend, account direct vergrendeld	Laag, geen uitval	Niet meldplichtig, intern geregistreerd	3 nov	Extra controle op mailfilters

Waarom het logboek het bewijs is. Een auditor toetst opzet, bestaan en werking. De procedure bewijst de opzet en een oefening het bestaan, maar alleen een bijgehouden logboek bewijst dat het proces werkt. Noteer daarom elk incident, hoe klein ook.

Oefen voordat het nodig is

1. **Speel minstens eens per jaar een fictief incident na.** Van ontdekking tot melding, met de echte namen uit de wie-doet-wat-tabel en met de klok erbij.
2. **Noteer ook de oefening in het logboek.** Een geoefend proces is aantoonbaar werkend; dat is precies wat toezichthouder en auditor willen zien.
3. **Evalueer en stel bij.** Elke oefening en elk echt incident eindigt met de vraag wat er in de kolom Geleerd komt. Zo wordt melden een gewoonte in plaats van een crisis.

Verder met documenten.nl. Of de Cyberbeveiligingswet op u van toepassing is, toetst u met de NIS2 zelfevaluatie checklist (C2) uit de Toolbox. De samenhang tussen de kaders leest u op documenten.nl/compliancy.