



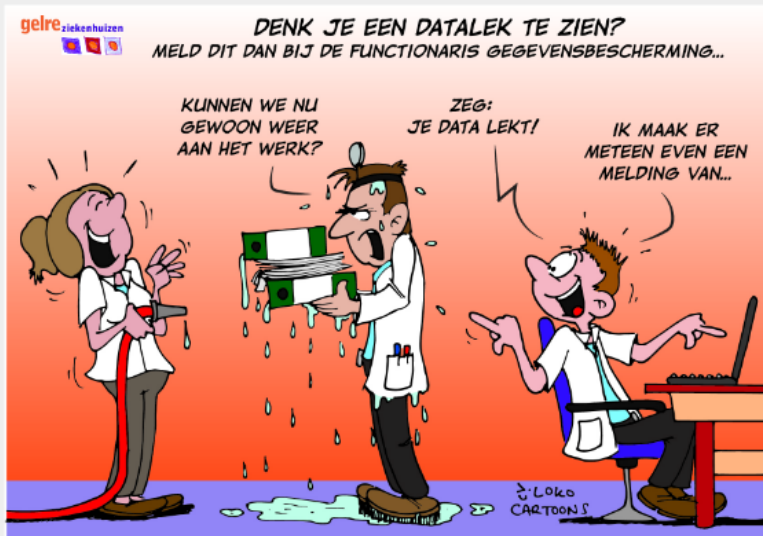
Meldplicht datalekken

'do's and dont's bij PostNL'

Jean Paul van Schoonhoven
Chief Privacy Officer
Cyber Security & Privacy Office (CSPO)

datalek@postnl.nl
privacy@postnl.nl
cybersecurity@postnl.nl

Ter illustratie



altijd goed lachen om anderen
terwijl....



'PostNL snapt internet niet'

Wat houdt de meldplicht in?

'Elke inbreuk op de beveiliging'
thans:

Artikel 34a Wet bescherming persoonsgegevens

vanaf 25 mei 2018:

Artikel 33 en 34 Algemene Verordening
Gegevensbescherming

Boeterisico?

Ja, huidige boetebevoegdheid van de Autoriteit Persoonsgegevens (AP) is
€820.000 of 10% van de omzet.

Per 25 mei 2018:
€20 miljoen of 4% wereldwijde omzet

Op basis van de huidige boetebeleidsregels van de AP is een schending van de meldplicht gemaximeerd
op €500.000 per overtreding.

Werkelijke kosten?

Op basis van jaarlijkse wereldwijde onderzoeken van Verizon en het Ponemon Institute blijkt dat een datalek gemiddeld €150 per record kost en dat de gemiddelde directe en indirecte kosten van een gemiddeld datalek ongeveer €3 tot €4 miljoen bedragen...

It takes 20 years to build a reputation and five minutes to ruin it. If you think about that, you'll do things differently.



Warren Buffett
American business magnate
QuoteHD.com (Born 1930)

Waaruit bestaat de meldplicht?

Wettelijke plicht om binnen 72 uur na ontdekking de AP te informeren. De meldbevoegdheid binnen PostNL ligt bij de CPO.

Wettelijke plicht om bij kans op nadelige gevolgen voor de betrokkenen, deze onverwijld te informeren.

Externe beleidsregels van de AP: Beleidsregels meldplicht datalekken (www.autoriteitpersoonsgegevens.nl)

Wat doet het CSPO van PostNL er aan?

1. Bewustwording stimuleren
2. Procesbeschrijving datalekken
3. BCP Datalekken en IT aanval
4. functionele mailbox datalek@postnl.nl
5. Informatie op postnl.nl

Impact voor de organisatie

- In de contracten met zakelijke relaties moet een bepaling rondom de procesgang bij een datalek zijn opgenomen.
- PostNL is voor het kernproces van vervoer geen bewerker in de zin van de Wbp maar een gedeelde verantwoordelijke.
- CSPO heeft een speciaal privacy addendum opgesteld als bijlage bij de zakelijke contracten.
- We hanteren een interne meldtermijn richting de klant van 48 uur. Dit geldt wederzijds ook voor de klant.
- Voor data die we namens de klant meer verwerken dan alleen NAW van de ontvanger, is PostNL in beginsel wel een bewerker. Hiervoor moet naast het privacy addendum een bewerkersovereenkomst worden gesloten.
- De templates van de bewerkersovereenkomst en het addendum worden beheerd door het CSPO. De inhoud er van wordt samen met Legal actueel gehouden. De templates zijn te vinden op de interne connect site van het CSPO.
- Legal is verantwoordelijk voor de onderhandelingen over contracten. Het CSPO is de escalatie jegens de klant bij discussie of als er beleidskeuzes gemaakt moeten worden.
- Autorisatiebeheer van de afdeling sluitend houden anders 'interne datalek'.
- Actieve informatievoorziening richting onze klanten organiseren over de rol van PostNL in de verwerkingen van persoonsgegevens.