Slechte waarschuwings-berichten na datalekken

Slachtoffers van datalekken lopen onnodig risico

Rapportage september 2024

AUTORITEIT
PERSOONSGEGEVENS

Inhoudsopgave

1. Samenvatting

Waarschuwingsberichten voldoen niet aan alle wettelijke vereisten

In de Algemene verordening gegevensbescherming (AVG) en de Richtlijn gegevensbescherming bij rechtshandhaving (RGR) staan eisen waaraan waarschuwingsberichten aan slachtoffers van datalekken moeten voldoen. Uit onderzoek van de Autoriteit Persoonsgegevens (AP) blijkt echter dat organisaties zich niet houden aan alle wettelijke vereisten. Zo zijn waarschuwingsberichten vaak onduidelijk, duurt het lang voordat ze het slachtoffer bereiken en benoemen organisaties de gevolgen van het datalek niet of onvoldoende.

Het belang van waarschuwingsberichten

Als een organisatie getroffen wordt door een datalek dat waarschijnlijk een hoog risico oplevert voor de rechten en vrijheden van slachtoffers, dan is de organisatie wettelijk verplicht het datalek te melden aan de slachtoffers. In een goed waarschuwingsbericht krijgen slachtoffers informatie over het datalek en waarschuwt de organisatie hen voor de mogelijke negatieve gevolgen van het datalek. Zijn er bijvoorbeeld contactgegevens gelekt? Dan moeten slachtoffers extra alert zijn op phishing. Toch blijkt uit diverse tips en klachten die binnenkomen bij de AP dat de kwaliteit van waarschuwingsberichten vaak nog tekortschiet. Ook in de media komt dit soort signalen naar voren. De AP heeft daarom onderzoek uitgevoerd naar de waarschuwingsberichten van de 53 grootste datalekken uit 2023.

Slechte waarschuwingsberichten hebben meerdere oorzaken

Waarschuwingsberichten kunnen om diverse redenen van lage kwaliteit zijn. Organisaties hebben tijdens het onderzoek aangegeven onvoldoende kennis te hebben van het schrijven van teksten in heldere taal. Ook leveren interne afstemming en onderzoek naar het datalek vertraging op bij het versturen van waarschuwingsberichten. Er lijkt ook een gebrek aan bewustzijn en kennis te zijn over de mogelijke gevolgen van datalekken.

De AP publiceert aanbevelingen

De AP ziet een lage kwaliteit van waarschuwingsberichten als een groot risico. Daarom is er op de website van de AP informatie met aanbevelingen en voorbeelden beschikbaar voor organisaties. De AP beschrijft de meest gemaakte fouten en laat zien wat er in goede waarschuwingsberichten staat. Om de kwaliteit van waarschuwingsberichten te verbeteren, zal de AP ook strenger controleren op de inhoud van de berichten. Wanneer organisaties slachtoffers onvoldoende of onjuist informeren, neemt de AP contact op met deze organisaties.

De aanbevelingen staan op de website van de AP:
www.autoriteitpersoonsgegevens.nl/themas/beveiliging/datalekken/zo-informeert-u-slachtoffers-over-een-datalek

2. Lage kwaliteit waarschuwingsberichten

In het kort

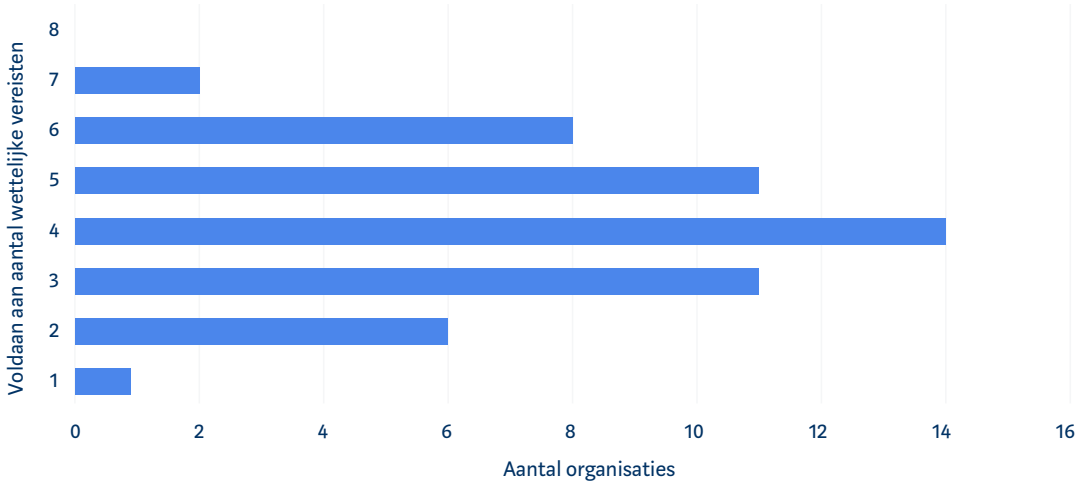
- Van de 53 onderzochte organisaties heeft geen enkele zich gehouden aan alle wettelijke vereisten voor een waarschuwingsbericht.
- Het slechtst scorende onderdeel van waarschuwingsberichten is de helderheid van de tekst. Van de 53 organisaties scoorde 64% hier een onvoldoende voor.
- Waarschuwingsberichten worden vaak te laat verzonden.

Beoordeling van de waarschuwingsberichten

In dit onderzoek zijn de 53 datalekken uit 2023 met het hoogste aantal geïnformeerde slachtoffers onderzocht. Deze 53 datalekken hebben in totaal geleid tot 26.140.791 individuele waarschuwingsberichten aan Nederlandse of buitenlandse slachtoffers. Hierbij kan dezelfde persoon slachtoffer zijn van meerdere datalekken en dus meerdere waarschuwingsberichten ontvangen. Van de 53 datalekken waren er 32 het gevolg van cybercriminaliteit (hacking, malware en phishing).

De waarschuwingsberichten zijn beoordeeld op acht beoordelingscriteria: de wettelijke vereisten. De beoordelingscriteria zijn afkomstig uit de AVG en staan in de bijlage van dit rapport. In figuur 1 is te zien voor hoeveel wettelijke vereisten organisaties een voldoende hebben gescoord. Geen enkele organisatie heeft voldaan aan alle wettelijke vereisten. Slechts twee organisaties voldeden aan zeven van de acht criteria. Ook is te zien dat een groot deel van de organisaties slechts de helft van de wettelijke vereisten had verwerkt in waarschuwingsberichten. Dit heeft tot gevolg dat slachtoffers van datalekken kwetsbaar blijven voor oplichting, identiteitsfraude of andere negatieve gevolgen. Bepaalde groepen mensen, zoals ouderen, lopen hierdoor extra risico.

FIGUUR 1 AANTAL WETTELIJKE VEREISTEN WAAR ORGANISATIES AAN HEBBEN VOLDAAN



Waar bestaat een goed waarschuwingsbericht uit?

Een goed waarschuwingsbericht bevat tenminste deze onderdelen:

- een beschrijving van de gelekte gegevens;
- een beschrijving van wat er is gebeurd;
- een beschrijving van de waarschijnlijke gevolgen voor slachtoffers;
- een passend advies over wat slachtoffers kunnen doen;
- een beschrijving van de (voorgenomen) maatregelen door de organisatie;
- een contactpunt voor slachtoffers die vragen hebben.

Bovendien moet de tekst in heldere, begrijpelijke taal zijn geschreven en moet de organisatie zonder onnodige vertraging communiceren met de slachtoffers.

TABEL 1 SCORE PER CRITERIUM

Plaats	Onderdeel	Onvoldoende (% van organisaties)
1.	Heldere taal	64%
2.	Snelle communicatie	58%
3.	Benoeming waarschijnlijke gevolgen	57%
4.	Benoeming getroffen maatregelen	57%
5.	Duidelijkheid gelekte gegevens	47%
6.	Duidelijke beschrijving datalek	43%
7.	Benoeming passend advies	34%
8.	Contactpunt voor vragen	26%

Beoordeling per onderdeel

Uit de beoordeling van de 53 datalekken en waarschuwingsberichten blijkt dat waarschuwingsberichten het slechtst scoren op heldere taal. Bovendien communiceren organisaties vaak te traag. Het benoemen van de mogelijke gevolgen voor slachtoffers en de (voorgenomen) maatregelen door organisaties blijkt ook een lastig onderdeel. Ten slotte benoemde slechts ongeveer de helft van de onderzochte organisaties duidelijk welke gegevens er waren gelekt.

Van de 53 datalekken was er bij 35 datalekken een passend advies aan de slachtoffers. Bij deze datalekken hebben echter slechts 9 van de 35 organisaties een waarschuwingsbericht binnen 7 dagen verstuurd. Gemiddeld deden de 35 organisaties er zelfs 23 dagen over om een waarschuwingsbericht te versturen. Dit betekent dat organisaties slachtoffers gemiddeld pas na 23 dagen wezen op de actie die zij konden ondernemen. In die tijd kunnen criminelen al misbruik maken van de gelekte gegevens en mensen oplichten. In de AVG staat geen exacte termijn waarbinnen een organisatie slachtoffers moet informeren. Wel zijn organisaties verplicht om een datalek "onverwijld" te melden aan slachtoffers.

3. Oorzaken van lage kwaliteit

In het kort

- Organisaties hebben onvoldoende kennis van het schrijven van teksten in heldere taal.
- Organisaties willen vaak eerst onderzoek naar het datalek afwachten, terwijl slachtoffers juist baat hebben bij vlugge communicatie.
- Interne afstemming zorgt vaak voor vertraging bij het versturen van waarschuwingsberichten.
- Er is onvoldoende kennis en bewustzijn over de mogelijke gevolgen van een datalek voor slachtoffers.

Moeite met het schrijven in heldere taal

Uit dit onderzoek blijkt dat organisaties vaak moeite hebben met het schrijven van waarschuwingsberichten in heldere taal. Organisaties hebben daar vaak onvoldoende kennis van, of zijn zich niet bewust van hun (te hoge) taalniveau. Dit kan betekenen dat niet alle slachtoffers voldoende begrijpen wat er met hun persoonsgegevens is gebeurd en wat ze nu precies moeten doen. Bovendien hebben organisaties de neiging om vaktaal te gebruiken en hebben zij soms onvoldoende kennis van het taalniveau van slachtoffers.

Het dilemma: onderzoek afwachten of onvolledige informatie geven?

Organisaties hebben aangegeven dat zij bij datalekken onderzoek naar het datalek willen afwachten voordat zij de slachtoffers informeren. Hierbij speelt een dilemma: moet je als organisatie de slachtoffers pas informeren als je alle informatie hebt? Of moet je slachtoffers al eerder informeren? Slachtoffers zijn dan sneller gewaarschuwd, maar het risico is dat zij onjuiste of onvolledige informatie krijgen. Voor slachtoffers staat voorop om snel informatie te krijgen, zodat zij voorzorgsmaatregelen kunnen nemen tegen schade of verdere inbreuken op de privacy. De AP adviseert om wel zo transparant mogelijk te zijn over onduidelijkheden en lopende onderzoeken. Slachtoffers ontvangen dan bijvoorbeeld een voorlopig waarschuwingsbericht, zodat zij alert zijn. Zodra een onderzoek is afgerond, kan de organisatie een vervolgbericht sturen met de definitieve bevindingen, zodat slachtoffers zichzelf nog beter kunnen beschermen.

Interne afstemming als vertragingsfactor

Gezien de gevoeligheid van datalekken vindt er in grote organisaties vaak veel afstemming plaats over waarschuwingsberichten, bijvoorbeeld met de functionaris gegevensbescherming, privacy officer en leidinggevenden. Organisaties geven aan dat zij deze interne afstemming vaak ervaren als vertragingsfactor.

Onvoldoende kennis van mogelijke gevolgen voor slachtoffers

In waarschuwingsberichten moeten organisaties de slachtoffers van een datalek niet alleen wijzen op de details van het datalek, maar ook op de mogelijke gevolgen. Wat kunnen criminelen bijvoorbeeld doen met een e-mailadres? Waarom is het zo ernstig als kopieën van identiteitsbewijzen lekken? Een duidelijke uitleg van de mogelijke gevolgen is van belang, zodat slachtoffers goed begrijpen hoe hun persoonsgegevens misbruikt kunnen worden. Om slachtoffers helder te informeren over de mogelijke gevolgen, is vanuit de organisatie basiskennis vereist over de risico's van datalekken. Hoewel deze informatie beschikbaar is, ook op de website van de AP, blijkt dat organisaties toch niet altijd voldoende communiceren over de mogelijke gevolgen. Dit komt door een gebrek aan kennis van het onderwerp en een gebrek aan bewustzijn. Organisaties denken zelf dat zij voldoende informeren over de mogelijke gevolgen, terwijl dit in de praktijk niet zo is.

De informatie in dit hoofdstuk is gebaseerd op een anonieme enquête die is uitgezet bij 48 van de 53 organisaties. De organisaties die buiten de EU waren gevestigd, hebben geen enquête ontvangen. De respons bedroeg 58%: 28 organisaties stuurden de vragenlijst retour.

4. De AP publiceert aanbevelingen

In het kort

- De AP publiceert aanbevelingen voor het opstellen van waarschuwingsberichten.
- Organisaties blijven zelf verantwoordelijk voor het naleven van de wet.

Wat gaat de AP doen?
Naar aanleiding van dit onderzoek heeft de AP aan de organisaties gevraagd hoe de AP hen beter zou kunnen helpen. Veel organisaties gaven aan dat zij behoefte hebben aan voorbeelden. Daarom zijn er op de website van de AP aanbevelingen met voorbeeldteksten beschikbaar. Deze aanbevelingen bieden organisaties houvast bij het schrijven van waarschuwingsberichten. De AP benadrukt in de aanbevelingen het belang van een goed waarschuwingsbericht. Bovendien legt de AP bij elk onderdeel van een waarschuwingsbericht uit welke fouten organisaties vaak maken, en hoe zij deze fouten kunnen voorkomen.

Zie: autoriteitpersoonsgegevens.nl/informeren-slachtoffers-datalek

Verantwoordelijkheid van organisaties
Organisaties blijven zelf verantwoordelijk voor de kwaliteit van hun waarschuwingsberichten. De berichten blijven namelijk maatwerk. Geen enkel datalek is hetzelfde en de mogelijke gevolgen kunnen sterk uiteenlopen. Zo zorgt een datalek waarbij alleen contactgegevens zijn gelekt voor andere risico's dan een datalek waarbij ook kopieën van identiteitsbewijzen zijn gelekt. En zo zal een ouderen-instelling cliënten op een andere manier willen informeren dan een webwinkel klanten informeert. De AP verwacht daarom altijd van organisaties dat zij zelf een onderbouwde risico-inschatting maken en de aanbevelingen van de AP toepassen op hun eigen situatie.

5. Strenger toezicht door de AP

In het kort

- De AP gaat de kwaliteit van waarschuwingsberichten strenger controleren.
- De AP zal voornamelijk organisaties corrigeren op waarschuwingsberichten die van lage kwaliteit zijn. Zo kunnen slachtoffers toch binnen korte termijn voldoende informatie krijgen.

Strengere controle

Het doel van het toezicht van de AP is dat mensen beter worden geïnformeerd over wat er met hun persoonsgegevens gebeurt. En dat zij weten wat zij kunnen doen om zichzelf te beschermen. Bij datalekken maakt dat slachtoffers weerbaarder. Hiervoor moet de kwaliteit van waarschuwingsberichten omhoog. De AP verwacht dan ook van organisaties dat zij de kwaliteit van waarschuwingsberichten verbeteren waar nodig.

De AP gaat de kwaliteit van waarschuwingsberichten intensiever controleren. Het belang van de slachtoffers staat hierbij voorop. Lopen slachtoffers onnodig of extra risico vanwege de lage kwaliteit van het waarschuwingsbericht? Dan treedt de AP op. In sommige gevallen doet de AP dat door een gesprek te voeren met de organisatie voor een snelle verbeterslag. In andere gevallen kan de AP een handhavingstraject starten en onderzoek doen.

Getroffen door datalek

Miryam kreeg een nep-betaalverzoek van de school van haar zoon

Begin 2024 werd Miryam door de school van haar zoon geïnformeerd dat zijn persoonsgegevens waren betrokken bij een cyberaanval. *"Dit waarschuwingsbericht wees mij op de mogelijke gevolgen van het datalek, zoals het ontvangen van phishingmails."* Een paar dagen later kreeg Miryam via de mail een betaalverzoek dat afkomstig leek van de school van haar zoon. *"In deze mail stond dat ik nog moest betalen voor het schoolkamp van mijn zoon. De mail was aan mij gericht en bevatte ook de naam en onderwijsinstelling van mijn zoon. Het leek daarom net echt. Door het eerdere waarschuwingsbericht van de school was ik extra alert en heb ik de betaallink niet geopend. Na afloop bleek het om phishing te gaan. Als ik erop had geklikt, was ik opgelicht."*

Miryam diende een tip in bij de AP, waarna de AP contact opnam met de organisatie waar het datalek had plaatsgevonden. De organisatie heeft toen de slachtoffers nogmaals specifiek gewaarschuwd voor dit soort oplichtingspogingen.

6. Bijlagen

Van de 53 onderzochte organisaties, stuurden slechts 22 organisaties een waarschuwingsbericht binnen 7 dagen na ontdekken van het datalek. 30 organisaties deden er langer over en 15 organisaties verstuurden pas na 22 dagen of meer hun waarschuwingsberichten. Bij de organisatie die er het langste over deed, duurde het 119 dagen. Van één organisatie is de datum van versturen van de waarschuwingsberichten onbekend, deze organisatie is om die reden uit deze statistieken gehouden.

TABEL 2 SNELHEID VAN COMMUNICATIE RICHTING SLACHTOFFERS VAN DATALEKKEN

Termijn	Aantal organisaties	Percentage (afgerond)
0 – 7 dagen	22	42%
8 – 14 dagen	10	19%
15 – 21 dagen	5	9%
22 dagen of meer	14	28%

Beoordelingscriteria met wettelijke herkomst

De waarschuwingsberichten zijn beoordeeld met behulp van de onderstaande tabel. De wettelijke criteria zijn gebaseerd op de **artikelen 12, 33 en 34 van de AVG, en overweging 86**.

TABEL 3

Beoordelingscriteria
1. Is het duidelijk welke gegevens (mogelijk) zijn gelekt? **Artikel 34, lid 2, AVG** - De in lid 1 van dit artikel bedoelde mededeling aan de betrokkene bevat een omschrijving, in duidelijke en eenvoudige taal, van de aard van de inbreuk in verband met persoonsgegevens [...]
2. Wordt op een duidelijke en volledige manier beschreven wat er is gebeurd? **Artikel 34, lid 2, AVG** - De in lid 1 van dit artikel bedoelde mededeling aan de betrokkene bevat een omschrijving, in duidelijke en eenvoudige taal, van de aard van de inbreuk in verband met persoonsgegevens [...]
3. Worden de waarschijnlijke gevolgen voor slachtoffers vermeld? **Artikel 34, lid 2, AVG** - De in lid 1 van dit artikel bedoelde mededeling aan de betrokkene bevat [...] ten minste de in artikel 33, lid 3, onder b), c) en d), bedoelde gegevens en maatregelen **Artikel 33, lid 3, AVG** - In de in lid 1 bedoelde melding wordt ten minste het volgende omschreven of meegedeeld: [...] c. de waarschijnlijke gevolgen van de inbreuk in verband met persoonsgegevens; [...]
4. 4. Wordt er een (passend) advies voorgeschreven voor slachtoffers? **Overweging 86, AVG** - [...] De kennisgeving dient zowel de aard van de inbreuk in verband met persoonsgegevens te vermelden als aanbevelingen over hoe de natuurlijke persoon in kwestie mogelijke negatieve gevolgen kan beperken.
5. Is het duidelijk welke maatregelen voorgesteld worden of reeds getroffen zijn door de organisatie? **Artikel 34, lid 2, AVG** - De in lid 1 van dit artikel bedoelde mededeling aan de betrokkene bevat [...] ten minste de in artikel 33, lid 3, onder b), c) en d), bedoelde gegevens en maatregelen **Artikel 33, lid 3, AVG** - In de in lid 1 bedoelde melding wordt ten minste het volgende omschreven of meegedeeld: [...] d. de maatregelen die de verwerkingsverantwoordelijke heeft voorgesteld of genomen om de inbreuk in verband met persoonsgegevens aan te pakken, waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan.
6. Is de melding in heldere taal geschreven? **Artikel 34, lid 2, AVG** - De in lid 1 van dit artikel bedoelde mededeling aan de betrokkene bevat een omschrijving, in duidelijke en eenvoudige taal, van de aard van de inbreuk in verband met persoonsgegevens [...]
7. Wordt er vermeld waar slachtoffers terecht kunnen met vragen? **Artikel 34, lid 2, AVG** - De in lid 1 van dit artikel bedoelde mededeling aan de betrokkene bevat [...] ten minste de in artikel 33, lid 3, onder b), c) en d), bedoelde gegevens en maatregelen **Artikel 33, lid 3, AVG** - In de in lid 1 bedoelde melding wordt ten minste het volgende omschreven of meegedeeld: [...] b. de naam en de contactgegevens van de functionaris voor gegevensbescherming of een ander contactpunt waar meer informatie kan worden verkregen; [...]
8. Is zo snel als redelijkerwijs mogelijk gecommuniceerd met slachtoffers? **Artikel 34, lid 1, AVG** - Wanneer de inbreuk in verband met persoonsgegevens waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen, deelt de verwerkingsverantwoordelijke de betrokkene de inbreuk in verband met persoonsgegevens onverwijld mee.

AUTORITEIT
PERSOONSGEGEVENS