Doorn en Keizer
Employment Lawyers • Arbeidsrechtadvocaten

DenK

Meldplicht datalekken en het nieuwe boetebeleid: hoe goed is uw onderneming voorbereid?

HR Seminar 26 mei 2016

'200.000 e-mailadressen gestolen uit database Philips'

Usb-stick ministerie op straat

TelSell bevestigt diefstal creditcardgegevens

Sites NPO en radiostations lekken gegevens 2,3 miljoen mensen

PANAMA PAPERS
Onthullingen uit de verborgen wereld van belastingparadijzen

NS stuurde duizenden bankgegevens per ongeluk op aan klanten

T-Mobile personeel verkoopt klantgegevens

Rechter vergeet koffer met dossiers in trein

Inhoudsopgave

DenK

1. Wet Bescherming Persoonsgegevens

Onderwerp	Uitleg	Voorbeelden/opmerkingen
Wat?	1. Persoonsgegevens: info over persoon of herleidbaar tot persoon. 2. Bijzondere persoonsgegevens: info over godsdienst/levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap van een vakvereniging en strafrechtelijk verleden. 3. Verwerken: elke handeling m.b.t. persoonsgegevens.	
Wie?	1. Betrokkene: degene op wie persoonsgegeven betrekking heeft. 2. Verantwoordelijke: degene die bepaalt dat en hoe persoonsgegevens worden verwerkt. 3. Bewerker: degene die t.b.v. verantwoordelijke gegevens verwerkt. 4. Toezichthouder: Autoriteit Persoonsgegevens.	
Hoe?	Zorgvuldig, doelbinding, grondslagen, kwaliteit, **beveiliging**, bewaren, meldingsplicht (toezichthouder), informatieplicht (betrokkene), **meldplicht datalekken** en rechten van betrokkene.	**Beveiliging.** Verplichting technische en organisatorische beveiligingsmaatregelen te nemen tegen verlies of onrechtmatige verwerking (artikel 13 Wbp). **Meldplicht datalekken.** Wet meldplicht datalekken en uitbreiding boetebevoegdheid (1 januari 2016), beleidsregels meldplicht en boetebeleid.

2. Wat is een datalek? (1)

Onderwerp	Uitleg	Voorbeelden/opmerkingen
Beveiligingsincident	Inbreuk beveiliging waarbij: 1. persoonsgegevens raken verloren; of 2. onrechtmatige verwerking persoonsgegevens redelijkerwijs niet kan worden uitgesloten (artikel 34a Wbp).	Onrechtmatige verwerking: o.m. aanpassen of veranderen van persoonsgegevens en onbevoegde toegang tot, of afgifte daarvan. Inbreuk kan bestaan uit: - Tekortschieten, omzeilen of onjuiste toepassing beveiligingsmaatregelen. - Menselijke fouten verantwoordelijke of bewerker. Bronnen van inbreuk: - Verlies of diefstal. - Kwaadwillende insider of buitenstaander (hacker of activist).

2. Wat is een datalek? (2)

2. Wat is een datalek? (3)

2. Wanneer moet u een datalek melden aan de Autoriteit Persoonsgegevens? (1)

Onderwerp	Uitleg	Voorbeelden/opmerkingen
Wat?	Datalek “leidt tot de aanzienlijke kans op **ernstige nadelige gevolgen** dan wel ernstige nadelige gevolgen heeft **voor de bescherming van persoonsgegevens**” (artikel 34a Wbp).	
	Factoren, persoonsgegevens van “gevoelige aard”, waaronder: - bijzondere persoonsgegevens; - financiële gegevens; - gegevens die kunnen leiden tot stigmatisering of uitsluiting betrokkene; - gebruikersnamen, wachtwoorden en inlognamen; - gegevens die kunnen worden misbruikt voor (identiteits)fraude; - gegevens in DNA-banken; - gegevens die onderworpen zijn aan geheimhouding en beroepsgeheim.	
	Overige factoren: - veel persoonsgegevens per persoon of gegevens van grote groep betrokkenen; - of ingrijpende beslissingen worden genomen met gegevens; - omvangrijke verwerkingen die in ketens worden verdeeld; - kwetsbare groepen; - hack.	

3. Wanneer moet u een datalek melden aan de Autoriteit Persoonsgegevens? (2)

Onderwerp	Uitleg	Voorbeelden/opmerkingen
Wie?	- Verantwoordelijke, ook in een keten met (sub)bewerkers blijf je eindverantwoordelijke. - Eigen beoordeling staat centraal, AP zal geen beoordeling geven. - Bewerker heeft geen meldplicht, maar partijen kunnen wel afspreken dat bewerker melding doet.	
Wanneer?	Onverwijld: zonder onnodige vertraging, en uiterlijk binnen 72 uur.	
Hoe?	Standaard webformulier te verkrijgen op website AP.	Melding bevat in ieder geval (artikel 34a lid 3 en lid 4 Wbp): - aard van de inbreuk; - instanties waar meer informatie over de inbreuk kan worden verkregen; - aanbevolen maatregelen om de negatieve gevolgen van de inbreuk te beperken; - beschrijving van geconstateerde en vermoedelijke gevolgen inbreuk voor verwerking van persoonsgegevens; en - maatregelen die verantwoordelijke heeft getroffen of voorstelt te treffen om deze gevolgen te verhelpen.

4. Wanneer moet u een datalek melden aan de betrokken personen? (1)

Onderwerp	Uitleg	Voorbeelden/opmerkingen
Wat?	Als datalek “waarschijnlijk **ongunstige gevolgen** zal hebben voor diens persoonlijke levenssfeer”.	Als melding aan AP wegens “ernstige nadelige gevolgen” of “aanzienlijke kans” daarop, dan in vele gevallen ook een melding aan betrokkene wegens “waarschijnlijk ongunstige gevolgen”. Omgekeerd idem.
	- Ongunstige gevolgen zijn bijvoorbeeld onrechtmatige publicatie, reputatieschade (‘aantasting eer en goede naam’), identiteitsfraude of discriminatie. - Als datalek gevoelige gegevens betreft, grote(re) kans dat er ongunstige gevolgen zijn. - Door kennisgeving kan betrokkene alert zijn op mogelijke gevolgen en indien mogelijk extra voorzorgsmaatregelen nemen (nieuw wachtwoord of dienst/product van andere partij afnemen).	
	Uitzonderingen op de meldplicht. Gegevens ‘ontoegankelijk of onbegrijpelijk’ (artikel 34a lid 6 Wbp): gegevens zijn onleesbaar: - zijn de gegevens blootgesteld aan vernietiging of aantasting? - waren de gegevens versleuteld op het moment van inbreuk? - is de versleuteling adequaat? - is het restrisico acceptabel?	Voorbeelden: versleutelen (encryptie), omzetten naar een unieke code (hashen) of op afstand verwijderen (remote wiping). 

4. Wanneer moet u een datalek melden aan de betrokken personen? (2)

Onderwerp	Uitleg	Voorbeelden/opmerkingen
Wie?	- Verantwoordelijke, ook in een keten met (sub)bewerkers blijf je eindverantwoordelijke. - Eigen beoordeling staat centraal, maar AP kan ook verlangen dat je alsnog meldt aan betrokkene. Dat is een bindende aanwijzing op straffe van een boete (artikel 34a lid 7 WBP). - Bewerker heeft geen meldplicht, maar partijen kunnen wel afspreken dat bewerker melding doet.	
Wanneer?	Onverwijld.	
Hoe?	- Vormvrij. - Doel is om zoveel mogelijk betrokkenen te bereiken om de gevolgen van een datalek zoveel mogelijk te beperken. - Melding bevat in ieder geval (artikel 34a lid 3 Wbp): (i) aard van de inbreuk; (ii) instanties waar meer informatie over de inbreuk kan worden verkregen; en (iii) aanbevolen maatregelen om de negatieve gevolgen van de inbreuk te beperken.	

4. Wanneer moet u een datalek melden aan de betrokken personen? (3)

VOORBEELD NOTIFICATIE

Belangrijke mededeling over databeveiliging
Leest u alstublieft het volledige bericht

Geachte,
Onze organisatie heeft ontdekt dat een ongeautoriseerde partij zich tussen *<datum>* en *<datum>* toegang heeft verschaft tot onze systemen. Zoals het er nu naar uitziet hebben de indringers toegang gehad tot *<omschrijving databases en functies>*. Hierbij is mogelijk persoonlijke informatie van u gecompromitteerd.

Het gaat hierbij om de volgende gegevens *<omschrijving categorieën persoons-gegevens>*. In reactie op deze inbreuk hebben wij de volgende stappen ondernomen:

1. Een extern erkende beveiligingsspecialist ingeschakeld om het lek grondig te onderzoeken en aanbevelingen te doen voor verbeteringen in de databeveiliging.
2. De betreffende dienst tijdelijk offline gehaald/ accounts op non actief gesteld/ gecompromitteerde bestanden geïsoleerd
3. Melding gemaakt van het lek bij de wettelijke toezichthouder: de Autoriteit persoonsgegevens

Op dit moment onderzoeken wij *<samen met eventuele derde IT specialist>* welke gegevens uit de systemen zijn ingezien of gedownload. Wij zullen u hierover zo snel mogelijk uitsluitsel geven. Wij geven u vandaag om *<tijdstip>* in ieder geval een nieuwe update over de stand van zaken.

Wij adviseren u in de tussentijd preventief de volgende stappen te ondernemen:

- Wijzig uw wachtwoord. U kunt dit eenvoudig doen via deze *link*.
- Indien u voor andere diensten gebruik maakt van hetzelfde wachtwoord, adviseren wij u ook deze wachtwoorden opnieuw in te stellen.

Wij betreuren deze inbreuk zeer en bieden onze excuses aan voor het ongemak dat dit voor u met zich meebrengt.
Mocht u vragen hebben naar aanleiding van deze mededeling, neemt u dan contact op met de klantenservice via <(gratis) telefoonnummer> of bekijk de website.

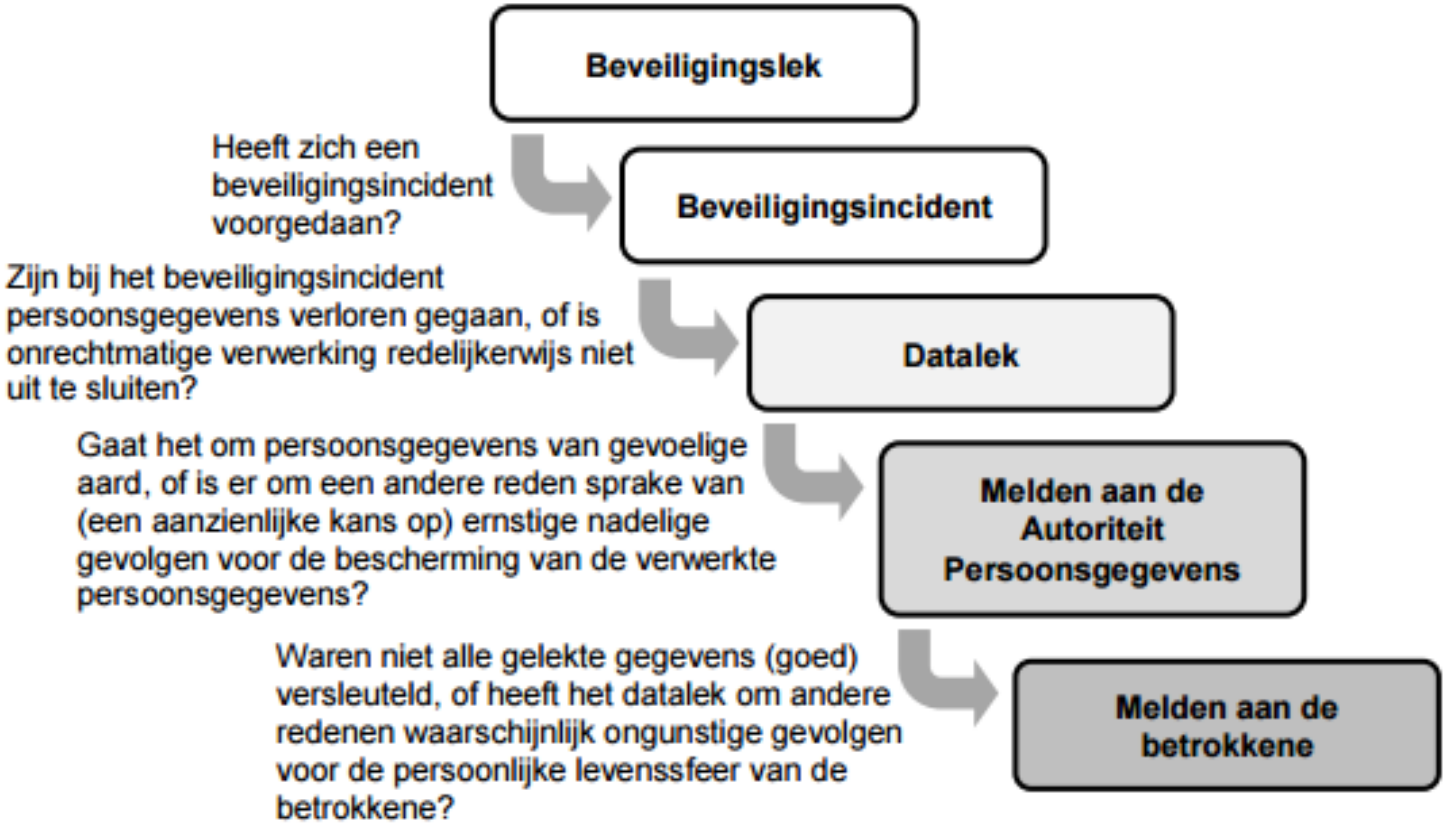
Groet,

DDMA (Data Driven Marketing Association)

5. Welke gegevens moet u vastleggen m.b.t. een datalek?

Onderwerp	Uitleg	Voorbeelden/opmerkingen
Documenteren	Verplichting om overzicht met gegevens datalek bewaren met daarin (artikel 34a lid 8 Wbp): (i) alle datalekken die onder meldplicht aan de AP vallen; (ii) feiten en gegevens omtrent aard inbreuk (bijv. oorzaak lek, soort gegevens, moment ontdekking, wijze waarop lek is gedicht), de instanties waar meer informatie kan worden verkregen en de aanbevolen maatregelen; en (iii) de tekst van de kennisgeving aan betrokkenen (indien van toepassing).	
	Bewaartermijn: minimaal 1 jaar.	

Tussenconclusie



6. Stand van zaken op dit moment? (1)

Onderwerp	Uitleg	Voorbeelden/opmerkingen
1500 meldingen per mei 2016	- Specifieke software selecteert op wat wel/niet actie behoeft (geen actie, wel gearchiveerd) - Actie: bij onzorgvuldig gedrag of nadere kennisgeving betrokkenen	- Verlies van niet-versleutelde apparaten (laptops, USB sticks, mobiele telefoons) - Onbeveiligd weggooien van informatie, zoals salarisinformatie in afvalcontainers - Onbeveiligde overdracht van gegevens, zoals medische data via onbeveiligde lijnen - Hackers die zich toegang verstrekken tot databases en deze versleutelen om vervolgens losgeld te vragen
2/3 nader bekeken of onderzoek gestart	Actie ondernomen tegen 70 organisaties: - Aanvullende rapportages - Opleggen verplichting om betrokkenen te informeren	Mogelijk voorkomen door: - Strengere beveiligingsregels en praktijken - Meer gebruik van geautomatiseerde systemen - Meer training
General Data Protection Regulation (GDPR) (Verordening Gegevensbescherming)	Op 25 mei 2018 van toepassing	Meldingen in NL indicatie wat er aan aantallen op Europees niveau
E-privacy Directive 2002/58/EC (Richtlijn privacy en electronische communicatie)	Bijzonder risico van inbreuken op de beveiliging van het netwerk: abonnees in kennis stellen + van de middelen om risico tegen te gaan + indicatie kosten	Commissie gaat Richtlijn herzien

7. Welke boetes kunnen er worden opgelegd? (1)

Onderwerp	Uitleg	Voorbeelden/opmerkingen
Hoogte boete	- Maximum: van max. € 4.500 (voor 1 januari 2016) naar max. € 820.000 of 10% nationale jaaromzet overtreder in voorgaande boekjaar (na 1 januari 2016). - Overtreding: Meldplicht aan AP/betrokkene = € 500.000, kennisgeving aan AP/betrokkene = € 200.000, bijhouden overzicht inbreuken = € 500.000, medewerkingsplicht = € 820.000 (of 10% nationale jaaromzet overtreder in voorgaande boekjaar).	Let op: in mei 2018 naar € 20 miljoen of 4% van wereldwijde omzet (art. 83 Algemene Verordening Persoonsgegevens). Voor niet-melden datalekken: € 20 miljoen of 2% van wereldwijde omzet.
Bindende aanwijzing	- Regel: AP geeft eerst bindende aanwijzing, waarin zij een termijn kan stellen waarbinnen aanwijzing moet worden gevolgd. - Uitzondering: AP legt direct boete op als overtreding opzettelijk is gepleegd of gevolg is van ernstig verwijtbare nalatigheid (artikel 66 lid 4 Wbp). - Boete: niet nakoming bindende aanwijzing = € 820.000 (of 10% nationale jaaromzet voorgaande boekjaar).	

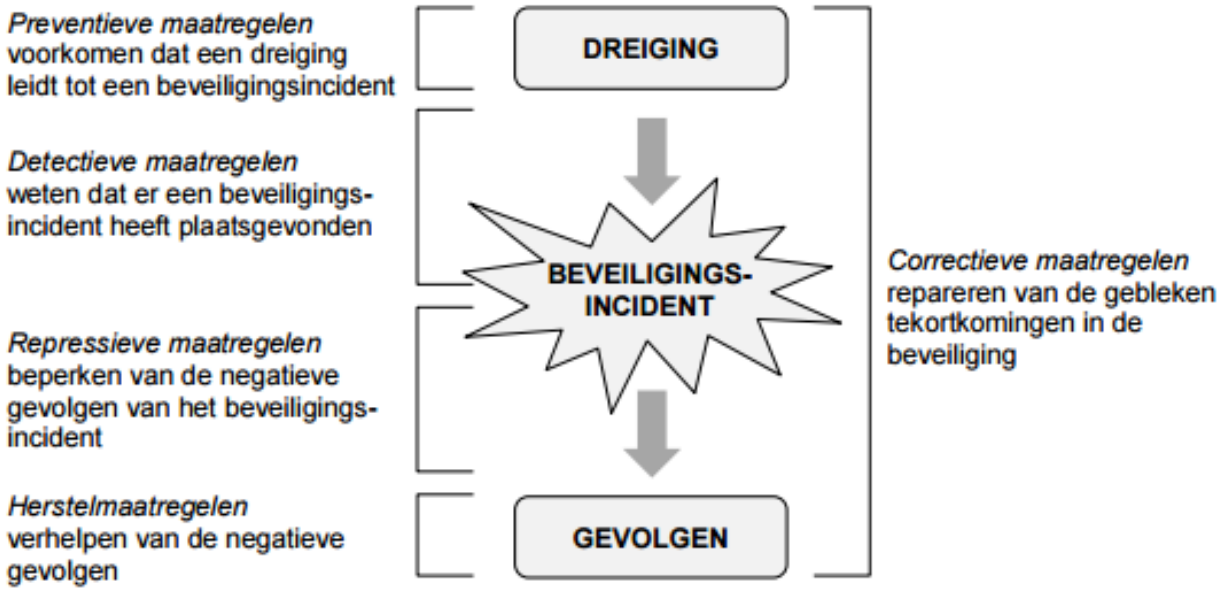
7. Welke boetes kunnen er worden opgelegd? (2)

Onderwerp	Uitleg	Voorbeelden/opmerkingen
Factoren van invloed zijn op hoogte boete	- Beoordeling ernst overtreding: aard en omvang, duur en impact op betrokkene en samenleving. - Beoordeling concrete omstandigheden: mate verwijtbaarheid overtreder, bij opzet of ernstig verwijtbare nalatigheid sprake van aanzienlijke mate van verwijtbaarheid. - Overige factoren: omstandigheden waaronder overtreding is gepleegd en (financiële) situatie overtreder.	
Boeteverhogende omstandigheden	- Bij recidive (dezelfde of vergelijkbare overtreding) verhoging van 50%. - Tegenwerken of belemmeren van onderzoek.	
Boeteverlagende omstandigheden	- Meer medewerking verlenen aan toezichthouder dan waartoe overtreder wettelijk verplicht is. - Uit eigen beweging overtreding beëindigd. - Uit eigen beweging slachtoffer schadeloos gesteld.	
Meerdere overtredingen	Bij meerdere, samenhangende, overtredingen kan - in plaats van afzonderlijke boete per overtreding - gezamenlijke boete voor alle overtredingen worden opgelegd.	
Hoogte boete niet passend	- Boete naast hogere categorie - Als €820.000 onvoldoende passend is, kan 10% van de nationale jaaromzet van de overtredende rechtspersoon	

8. Hoe kunt u zich voorbereiden op meldplicht datalekken? (1)

Onderwerp	Uitleg	Voorbeelden/opmerkingen
Privacybeleid	- Datastromen: wie, wat, waar, waarom en hoe? - Bewaartermijnen: hoelang, wie en waar? - Beveiliging: preventie, detectie, versleutelen en reparatie. - Meldplicht: actieplan, procedure omgang met en melding datalekken en (externe) communicatie. - Training: vergroot kenbaarheid (overtredingen) privacywetgeving.	
Inventarisatie bewerkers-overeenkomsten	Melding datalek-clausule, bewaartermijnen en aansprakelijkheid boetes.	
Verzekering	Huidige dekking controleren en evt. cyberrisico verzekering sluiten.	

8. Hoe kunt u zich voorbereiden op meldplicht datalekken? (2)



8. Hoe kunt u zich voorbereiden op meldplicht datalekken? (3)

STAP 1: DETECTEREN VAN EEN DATALEK

ACTIES

- Richt een meldpunt in.
- Maak een werkinstructie zodat medewerkers weten hoe ze moeten handelen.
- Controleer of u de juiste afspraken heeft gemaakt met eventuele bewerkers zodat u als verantwoordelijke aan uw zorgplicht kunt voldoen.

STAP 2: REGISTREREN VAN EEN DATALEK

ACTIE

Richt een incidentenregistratie in of breidt een bestaande incidentenregistratie uit conform de eisen uit de wet. Het overzicht bevat in ieder geval feiten en gegevens omtrent de aard van de inbreuk en de tekst van de kennisgeving aan de betrokkenen.

STAP 3: BEPALEN MELDPLICHT

U bent bewerker

ACTIE

Bepaal aan de hand van uw overeenkomst met de verantwoordelijke of en wanneer u het datalek bij de verantwoordelijke moet melden of eventueel rechtstreeks aan de Autoriteit Persoonsgegevens.

U bent verantwoordelijke

ACTIES

- Bepaal de aard van de gelekte gegevens
- Bepaal of u op basis van deze classificatie of u meldplichtig bent richting de Autoriteit Persoonsgegevens.
- Bent u meldplichtig? Meld uw datalek dan via het daarvoor bij de Autoriteit Persoonsgegevens beschikbare meldingsformulier.
- Verzamel (forensische) bewijsmateriaal en bewaar en registreren dit bij of in je incidentenregistratie.
- Specialistisch onderzoek doen en herstel uitvoeren: (forensisch) onderzoek en herstel kan zelf d.m.v. inzet van een particulier beveiligingsbureau of inschakelen van een instantie.

ACTIES

- Bepaal of u op basis van de classificatie of u meldplichtig bent richting betrokkene.
- Bent u meldplichtig? Meld uw datalek en richt indien nodig nazorg voor de betrokkenen in.

ACTIES

Van alle criminaliteit kunt u aangifte doen via het telefoonnummer 0900-8844 of bij uw lokale wijkteam. Van een aantal delicten kunt u ook online aangifte doen. https://www.politie.nl/themas/cybercrime.html of anoniem via https://www.meldknop.nl/misbruik/virtuele-diefstal/

STAP 4: DICHTEN VAN EEN DATALEK

ACTIES

- Bepaal waar het lek vandaan komt.
- Bepaal de omvang van het lek.
- Bepaal of het lek beheersbaar is; zo niet, schaal dan op naar de gangbare calamiteitenprocedure.
- Bepaal of er gerelateerde incidenten waarneembaar zijn.
- Zo ja, bepaal welke noodmaatregelen genomen kunnen worden.

STAP 5: BORGEN VAN VEILIGHEID

ACTIES

- Voer technische, organisatorische en beleidsmaatregelen door om het lek te dichten.
- Beschrijf de genomen maatregelen en registreren deze bij of in de incidentenregistratie.

HANDREIKING BESCHERMING PERSOONSGEGEVENS VOOR WATERSCHAPPEN

UNIE VAN WATERSCHAPPEN