
Operatie Datalek:
Is jouw organisatie veilig in dit digitale tijdperk?

09.20 Welkom
09.30 Olaf van Haperen
09.50 Marcel van Oirschot
10.10 Pauze
10.30 Maria Genova
11.15 Interactieve sessie, incl. lunch
11.15 – 11.45 ronde 1
11.55 – 12.25 ronde 2
12.35 – 13.05 ronde 3
12.30 Lunch
13.30 Afsluiting

Presentatie cyber risks, juridisch perspectief

TARQ: Operatie Datalek – 11 november 2016

KNEPPELHOUT
KORTHALS
ADVOCATEN

What tha hack?

KNEPPELHOUT
KORTHALS
ADVOCATEN

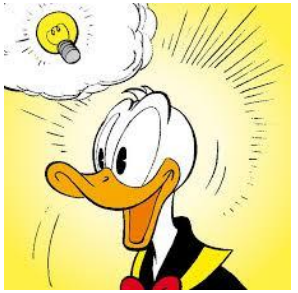
Privacy & Datalekken - actueel

- InHolland
- Mobiele datalekken kosten bedrijven gemiddeld €23,4 miljoen (Emerce, februari 2016)
- Identiteitsfraude ligt bij 53% aan basis van datalekken in 2015 (Emerce, februari 2016)
- Oude software is vragen om datalekken (Computable, april 2016)
- Gemeenten melden 147 datalekken bij toezichthouder (security.nl, 7 september 2016)
- Gegevens energiegebruik 2 miljoen huishoudens gestolen (nu.nl, 13 september 2016)
- Yahoo slachtoffer van mega-datalek: 500 miljoen accounts gestolen (nos.nl, 22 september 2016)
- Toch geen datalek bij gemeente Almelo (tweakers.net, 8 november 2016)
- Autoriteit Persoonsgegevens:

    - Niet alle datalekken worden gemeld (13 mei 2016)
    - Bijna 4000 datalekken gemeld sinds 1 januari 2016 (nos.nl, 7 oktober 2016)

Maar de verwachting was 66.000 meldingen op jaarbasis…?

Dus zegt de AP: “niet alle datalekken worden gemeld”……



KNEPPELHOUT
KORTHALS
ADVOCATEN

Wetten

- Wet bescherming persoonsgegevens → 1 september 2001
- Wet Meldplicht Datalekken → 1 januari 2016
- Algemeen Verordening Gegevensbescherming → 25 mei 2016

Compliant vanaf 25 mei 2018

- En ook:

- Beleidsregels AP 2015/2016
- Boetebeleidsregels → 16 januari 2016

KNEPPELHOUT
KORTHALS
ADVOCATEN

Juridische termen

- De “Verantwoordelijke” stelt doel en middelen vast van de verwerking van persoonsgegevens (art. 1 sub d Wbp)
- De “Bewerker” is degene die de verwerking uitvoert, zonder aan rechtstreeks gezag van de Verantwoordelijke te zijn onderworpen (art. 1 sub e Wbp)
- De Verantwoordelijke moet toezien op de naleving van de Wet meldplicht datalekken (art. 14 lid 1 Wbp)

Onder andere:

- Dus ook ervoor zorgen dat de bewerker maatregelen treft die nodig zijn om aan de meldplicht voor datalekken te kunnen voldoen (art. 14, lid 3 sub c Wbp)
- Bewerker heeft (nog) géén wettelijke meldplicht!
- Maar… in veel gevallen is de bewerker wèl de eerste die kennis krijgt van een opgetreden datalek!

Voorbeelden – Wat is een datalek?

Voorbeelden van datalekken (incidenten):

- een kwijtgeraakte USB-stick;
- een gestolen laptop;
- een inbraak door een hacker;
- een malware-besmetting;
- een calamiteit zoals een brand in een datacentrum.

Beleidsregels p. 20.

Melden[1]: Autoriteit Persoonsgegevens (1)

Meldplicht nr. 1: bij AP

- Verantwoordelijke eindverantwoordelijk voor melding!
- Bewerker moet de Verantwoordelijke tijdig en adequaat informeren over de datalekken waarvan hij kennis krijgt
- Melden incident, indien: *"… (aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van persoonsgegevens"* (art. 34a Wbp)

Melden[1]: Autoriteit Persoonsgegevens (2)

In ieder geval meldplicht wanneer de gegevens van gevoelige aard zijn:

- Bijzondere categorieën persoonsgegevens (raciale/etnische afkomst, politieke opvattingen, godsdienstige of levensbeschouwelijke overtuiging, etc.)
- Financiële gegevens
- Gegevens die kunnen leiden tot stigmatisering of uitsluiting
- Gebruikersnamen, wachtwoorden en andere inloggegevens
- Gegevens vatbaar voor ‘misbruik’ (identiteitsfraude)

Melden[1]: Autoriteit Persoonsgegevens (3)

Hoe en wanneer?

- Webformulier / fax
- *"Onverwijld"*, maar mag enige tijd nemen voor nader onderzoek…
- *"Zonder onnodige vertraging, en zo mogelijk niet later dan 72 uur na de ontdekking, […] tenzij op dat moment inmiddels al uit uw onderzoek is gebleken dat het incident niet onder de meldplicht datalekken valt. Indien u het incident later dan 72 uur na ontdekking aan de toezichthouder meldt, dan kunt u desgevraagd motiveren waarom u de melding later heeft gedaan."* (p. 31 Beleidsregels)

Melden²: Betrokkene (1)

Meldplicht nr. 2: Betrokkene (als er óók meldplicht bij AP bestaat)

- De overweging voor melding ook aan betrokkene

  "waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer" *(art. 34a lid 2 Wbp)*

  → onrechtmatige publicatie, aantasting eer/goede naam, ID-fraude, discriminatie, financiële schade

- Als Verantwoordelijke voldoende maatregelen genomen voor gegevensbescherming om melding aan betrokkene toch achterwege te kunnen laten?

Melden²: Betrokkene (2)

Dus is de vraag:

- Versleuteld?
  - Encryptie actief en up-to-date?
  - Encryptie / hashing niet gekraakt?
  - Conform ISO 27001-2 / NCSC / ENISA standaarden?
- Remote wipe mogelijk?
- Pseudonimisering (re-identificatie moeilijk gemaakt)?
- Restrisico acceptabel?
- Gegevens kwijt/vernietigd? Wèl schade voor Betrokkene = melden
- Persoonsgegevens van gevoelige aard = altijd melden

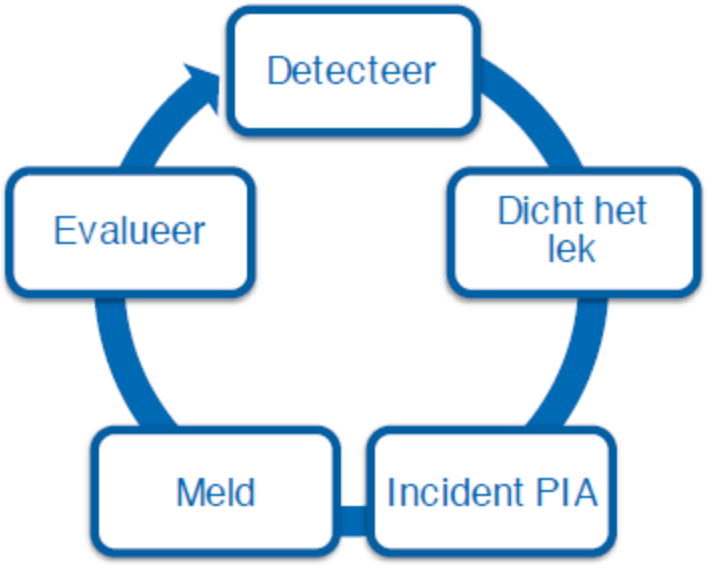
Melden²: Betrokkene (3)

Hoe en wanneer?

- *"Onverwijld"…* maar *"enige tijd voor onderzoek en voorbereiding behoorlijke zorgvuldige melding"* (art. 34a lid 2 Wbp / Beleidsregels p. 45)
- Betrokkene moet in staat gesteld worden maatregelen te nemen tegen schade
- Eerste melding om Betrokkene in gelegenheid te stellen wachtwoord te veranderen, zonder (nog) volledige details te geven

Melden: stappen (intern)

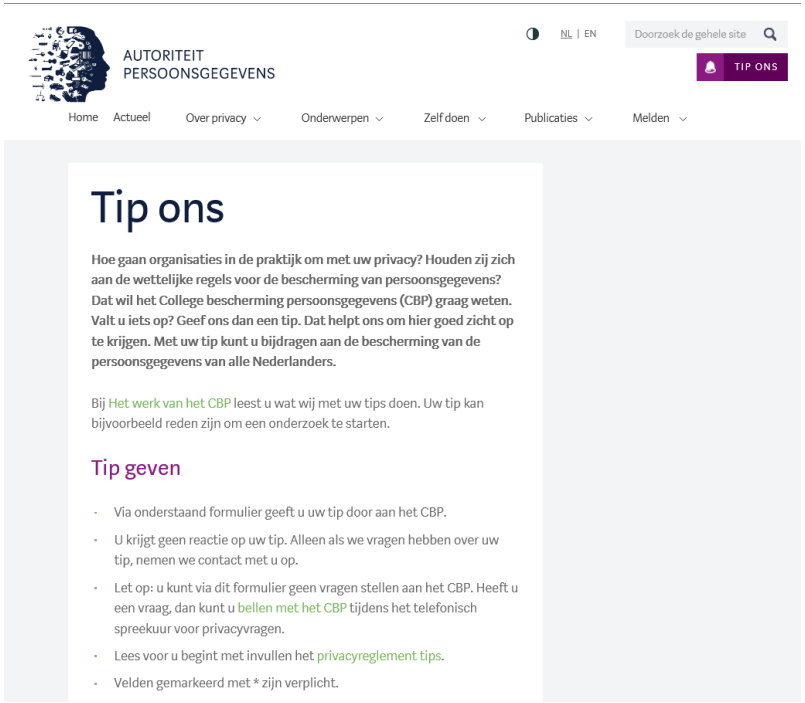
- Signaleer het lek
- Dicht het lek
- Privacy Impact Assessment
- Meld het lek
- Evalueer lek / meldproces
- Stel bij



KNEPPELHOUT
KORTHALS
ADVOCATEN

Niet melden?

Iedereen is toezichthouder! → reputatieschade?



KNEPPELHOUT
KORTHALS
ADVOCATEN

Data Protection Officer

KNEPPELHOUT
KORTHALS
ADVOCATEN

Stel je voor...

Zoals elke middag, ga je rond 12u30 naar de cafetaria van je bedrijf om met collega's te lunchen. Meteen merk je dat het gesprek onder de collega's deze middag geanimeerder is dan anders. Jan van human resources spreekt over een grondige oefening die zal moeten gebeuren, met de eventuele aanstelling van een DPO en het uitvoeren van een DPIA. Sofie van marketing reageert dat de invoering van de GDPR uitgebreide bevoegdheden voorziet voor de DPAs, met op Europees niveau een EDPB. Marc, de compliance officer, kijkt ernstig en mompelt dat gelet op de voorziene sancties, hij nu al immense druk ondervindt van het management om te zorgen dat het bedrijf in orde is met de nieuwe regels.

Jij hebt werkelijk geen idee waarover het gaat… DPO, DPIA, GDPR, … ?

Sancties?

AVG (GDPR) 2018 - handhaving vanaf 25 mei 2018

- Why: Privacyrichtlijn (95/46/EG) zorgde voor fragmentatie, rechtsonzekerheid, obstakels voor economische activiteit en verstoring concurrentie vs. toegenomen publieke aandacht voor bescherming individu.
- 170 (72) overwegingen, 94 (34) bepalingen en 26 (8) definities
- Activiteiten van verantwoordelijke **èn** bewerker
- Aanbieden van diensten aan betrokkenen in de EU of monitoren van hun gedragingen
- gedetailleerdere regels, meer verplichtingen voor verantwoordelijken en bewerkers, meer rechten voor betrokkenen, meer formaliteiten
- Geen meldplicht verwerking, maar accountability en documentatieplicht
- Ook meer bevoegdheden voor toezichthouders en hogere boetes (tot 4% / 20 miljoen)…

KNEPPELHOUT
KORTHALS
ADVOCATEN

Best Practices AVG

- Self-assessment: breng **datastromen** in kaart en weet wie toegang heeft tot die data (is die server in de VS echt noodzakelijk? Privacy Shield?).
- Doe (periodiek) een **PIA** in geval van high risk of nieuwe gegevensverwerking
- Pas bij implementatie van nieuwe processen/technieken het principe **Privacy-by-design** toe met **Privacy Enhanced Technologies** (PET)
- **Log** alles!
- Check of een **Data Protection Officer** vereist is voor uw organisatie
- Zorg dat betrokkenen net zo eenvoudig (als het aanleveren daarvan) hun gegevens kunnen inzien, wijzigen en verwijderen (**RtbF**)
- Zorg voor een up-to-date **draaiboek**

BEGINSELEN AVG

- **Rechtmatigheid**
- **Behoorlijkheid**
- **Transparantie**
- **Doelbinding**
- **Minimale gegevensverwerking**
- **Juistheid**
- **Opslagbeperking**
- **Integriteit en vertrouwen**
- **Verantwoording**

KNEPPELHOUT
KORTHALS
ADVOCATEN

Praktische consequenties?

- Awareness!!!
- Beleidsdocument voor informatiebeveiliging; draaiboek!!!
- Contracten checken / bewerkersovereenkomsten **nu** aanpassen → Bewerker heeft géén wettelijke verplichting om een datalek aan de Verantwoordelijke te melden
- Protocolplicht → vastleggen datalekken incl. meldingen AP/Betrokkenen → minimaal 1 jaar bewaren / 3 jaar indien gewichtige reden niet-informeren betrokkene
- Technische en organisatorische beveiligingsmaatregelen – twee-factor-authenticatie?
- Uitdiensttredingsprotocol
- En nog veel meer…

Vragen?

Olaf van Haperen
Managing partner / Advocaat
+ 31 6 17 45 62 99
oh@kneppelhout.nl

KNEPPELHOUT
KORTHALS
ADVOCATEN