De IT-jurist

Presentatie Jaarcongres ICT Accountancy
Overview Privacyrecht

André Kamps & Jan-Willem Oordt
De IT-Jurist bv
2 november 2016

De IT-jurist

Programma

- Korte introductie privacyrecht
- Rol accountant: verantwoordelijke of bewerker?
- Meldplicht Datalekken
- Europese Privacyverordening (Algemene Verordening Gegevensbescherming)
- Privacy Shield

De IT-jurist

Privacyrecht

- Wetgeving: Wet bescherming persoonsgegevens (Eur. Richtlijn 95/46/EG)
- Europese Privacyverordening 4 mei 2016 gepubliceerd, van toepassing vanaf 25 mei 2018
  - Meer harmonisatie, maar nog steeds veel nationale verschillen mogelijk
- Wetgeving bepaalt de wijze waarop er met persoonsgegevens mag worden omgegaan (verwerking)

Privacyrecht

- Verwerkingsproces heeft verschillende actoren:
  - Betrokkene, verantwoordelijke, bewerker (Privacyverordening: verwerker)

- Persoonsgegevens: gegevens die een natuurlijk persoon direct of indirect kunnen identificeren.

- Toezicht door Autoriteit Persoonsgegevens (AP, voorheen College Bescherming Persoonsgegevens)

- Wanneer mag je persoonsgegevens verwerken?

De IT-jurist

Privacyrecht

- **Verschillende grondslagen voor verwerking bijv:**
  - Gerechtvaardigd belang verantwoordelijke
  - Toestemming betrokkene
  - Noodzakelijk voor uitvoering overeenkomst
  - Noodzakelijk om wettelijke verplichting uit te oefenen
  - Noodzakelijk voor goede vervulling van een publiekrechtelijke taak door bestuursorgaan
  - Noodzakelijk ter vrijwaring van een vitaal belang van de betrokkene

Privacyrecht

- **Diverse verplichtingen van de verantwoordelijke:**
  - Doelbinding (geen ‘function creep’)
  - Beveiliging
  - Transport persoonsgegevens buiten de EU beperkt mogelijk
  - Bewerkersovereenkomst
  - Heeft u al een bewerkersovereenkomst gesloten?

Privacyrecht

❖ **Artikel 13 Wet bescherming persoonsgegevens:**

De verantwoordelijke legt passende technische en organisatorische maatregelen ten uitvoer om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich meebrengen. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.

Privacyrecht

- **Technische maatregelen:**
  - bijvoorbeeld versleuteling, firewall, etc.

- **Organisatorische maatregelen:**
  - bijvoorbeeld procedures, scheiden van functies, etc.

Laat zien dat je informatiebeveiligingsbeleid hebt en navolgt.

Privacyrecht

- **Rechten betrokkene**
  - Inzagerecht
  - Recht op correctie & aanvulling
  - Verwijderen persoonsgegevens op verzoek betrokkene? HVJ-EU, 13 mei 2014. (Google Spain) (Art. 10 WBP)
    - N.b. geen absoluut recht om vergeten te worden

De rol van de verantwoordelijke: beoordelen verzoek betrokkene

- Casus 1: Mevrouw X vs. Inspectie voor de Gezondheidszorg en Landelijk Meldpunt Zorg, verzoek tot verwijderen van klachtdossier met persoonsgegevens.
- Casus 2: Mevrouw Y vs. Gerechtsbestuur Hof ‘s-Hertogenbosch, verzoek tot verwijderen van procesdossiers met persoonsgegevens.

Accountant

- **Bewerkersovereenkomst voor accountants**
  - Soms bewerker, soms verantwoordelijke
  - NBA zegt het volgende:
  - In de regel een verantwoordelijke als u:
    - een opdracht uitvoert waarbij u een jaarrekening opstelt;
  - In de regel bent u een bewerker als u:
    - een verklaring verzekerd belang opstelt waarin persoonsgegevens zijn opgenomen.

Accountant

❖ Bewerker of verantwoordelijke (volgens NBA)

Type opdracht	Klant	Accountant
Standaard 100 – 999	Verantwoordelijke	Verantwoordelijke
Standaard 2000 – 2699	Verantwoordelijke	Verantwoordelijke
Standaard 3000 – 3850	Verantwoordelijke	Verantwoordelijke
Standaard 4400	Verantwoordelijke	Bewerker
Standaard 4410 (H)	Verantwoordelijke	Verantwoordelijke/bewerker
Opdrachten waar geen standaard van toepassing is (salarisadministraties)	Verantwoordelijke	Bewerker

Accountant

- **Bewerkersovereenkomst**
  - Van belang is om te beoordelen of u:
  - zelfstandig beslissingen moet kunnen nemen over het doel van de verwerking en de manier waarop u de verwerking uitvoert.
  - Zo ja, geen bewerkersovereenkomst met klant;
  - Wel met toeleveranciers:
  - Bijvoorbeeld softwareleveranciers, hostingbedrijven, etc.
  - NBA heeft een voorbeeld bewerkersovereenkomst (die getoetst is door De IT-jurist): accountant als bewerker.

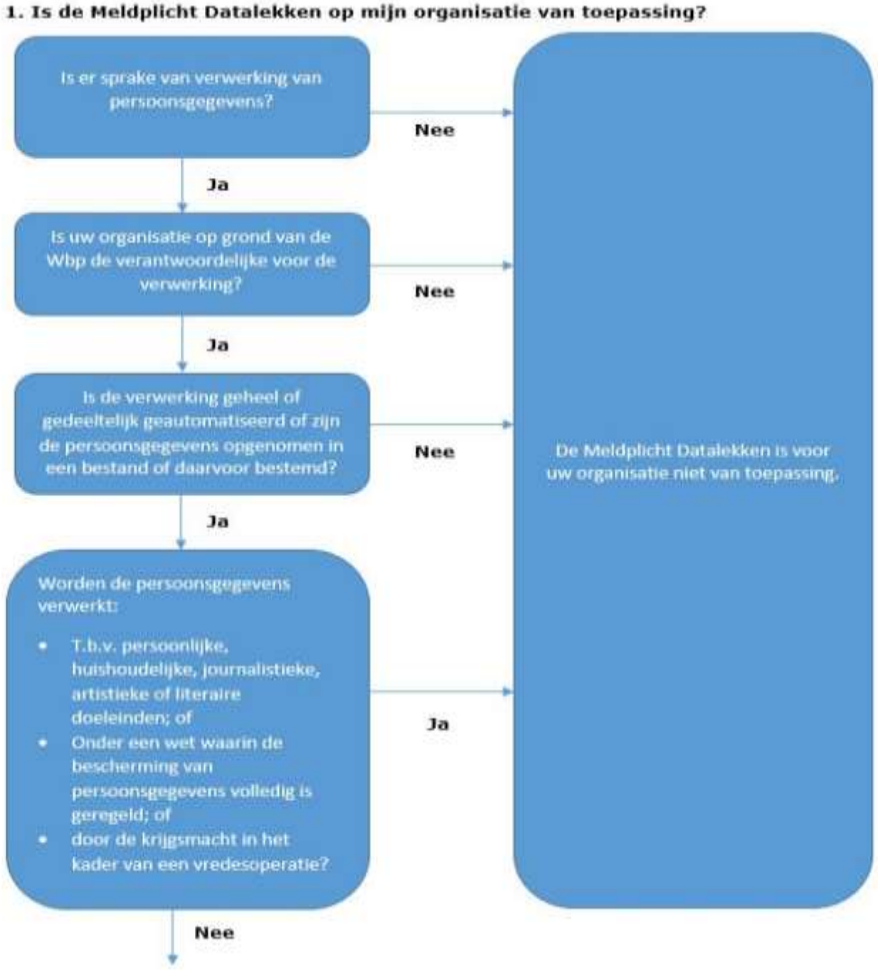
De IT-jurist

Meldplicht datalekken

- Meldplicht datalekken is sinds 1 januari 2016 van toepassing
- Beslisboom datalekken
- Rapport aan te vragen via GBNed

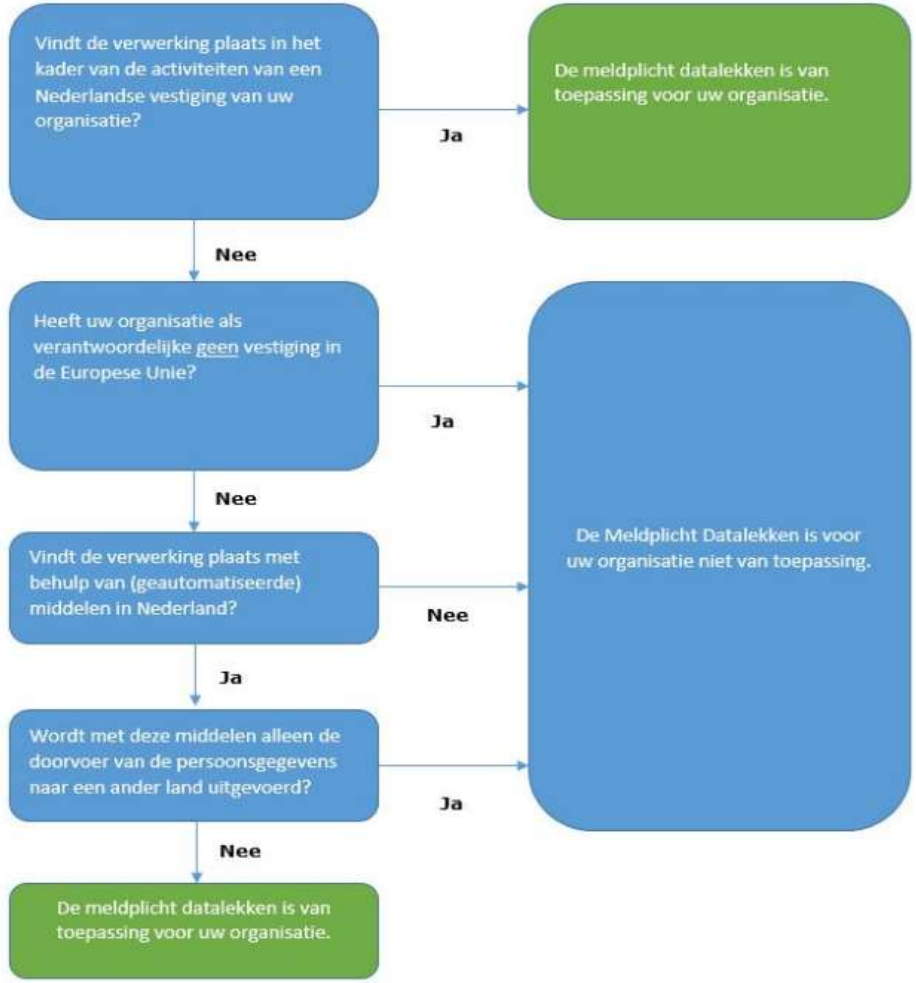
Meldplicht datalekken: Van toepassing voor uw organisatie?

- Er moet sprake zijn van verwerking van persoonsgegevens
- Meldplicht geldt voor de verantwoordelijke
- Geautomatiseerde verwerking of persoonsgegevens opgenomen in bestand?
- Geen uitzondering waardoor de Wbp buiten toepassing is?



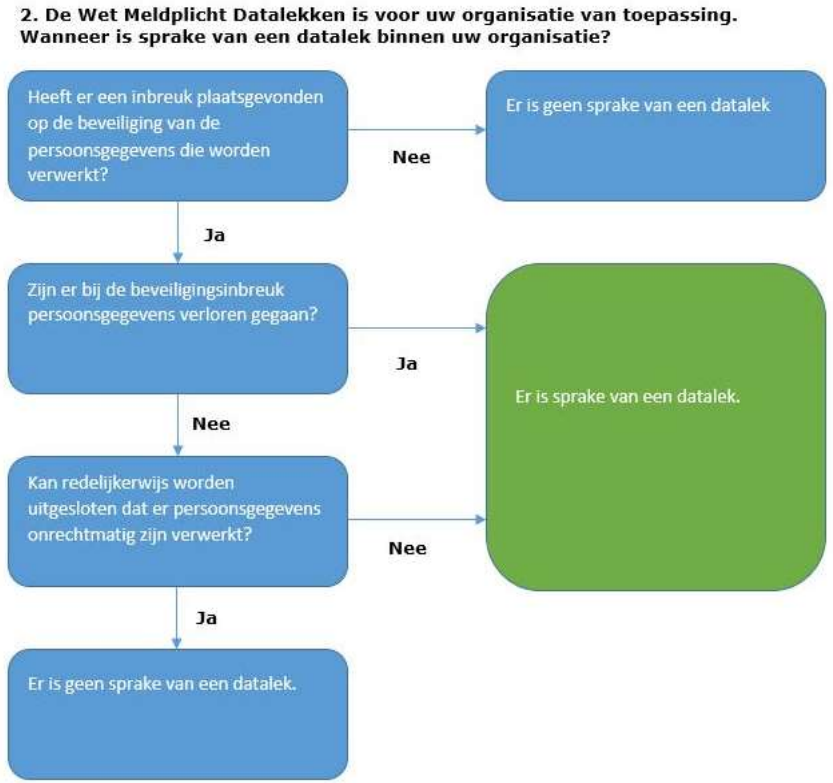
Meldplicht datalekken: Van toepassing voor uw organisatie? (2)

- Verwerking in Nederland?
- Geen verdere uitzonderingen?



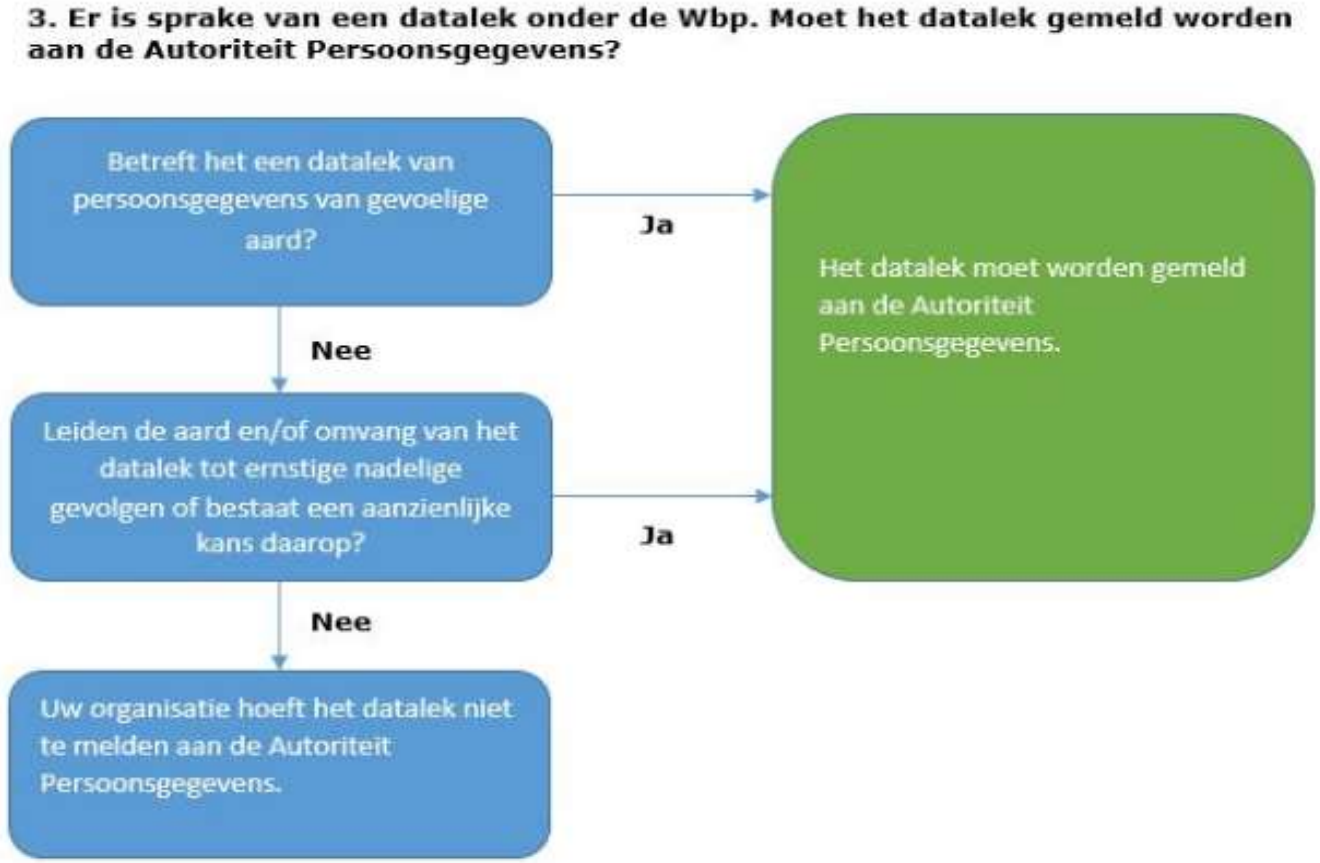
Meldplicht datalekken: Wanneer sprake van een datalek?

- Er moet sprake zijn van een inbreuk op de beveiliging
- Er moet sprake zijn van verlies van persoonsgegevens (en/of)
- Onrechtmatige verwerking van persoonsgegevens kan redelijkerwijs niet uit worden gesloten



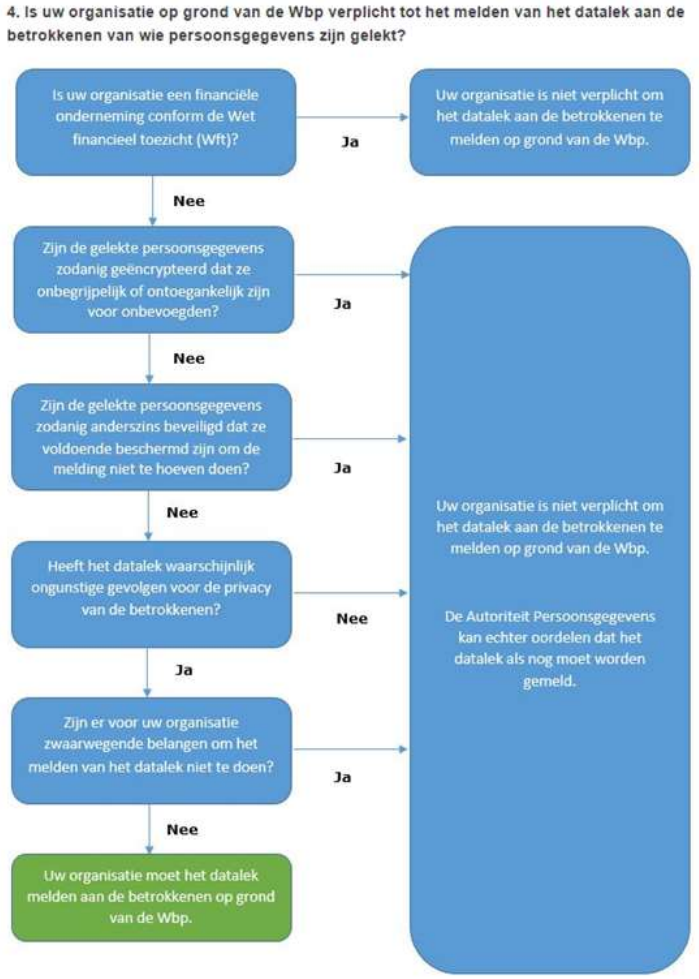
Meldplicht datalekken: Wanneer melden aan Autoriteit?

- Persoonsgegevens van gevoelige aard?
- (Kans op) ernstige nadelige gevolgen?
- “Onverwijld” melden



Meldplicht datalekken: Wanneer melden aan betrokkenen?

- Persoonsgegevens geëncrypteerd of anderszins voldoende beveiligd?
- Ongunstige gevolgen voor de privacy van betrokkenen?
- Zwaarwegende belangen om melden achterwege te laten?



Privacyverordening

- **Europese Privacyverordening**
  - Begrip persoonsgegeven uitgebreid: IP-adres, cookies
  - Wijziging geografische scope:
    - verwerking door activiteiten van een verantwoordelijke of verwerker in de EU, waarbij de verwerking plaatsvindt buiten de Unie;
    - verwerking door niet-EU verantwoordelijke of verwerker, indien:
      - Goederen en diensten worden aangeboden aan betrokkenen in EU;
      - Hij of zij gedrag monitort van betrokkenen, voor zover het gedrag in de Unie plaatsvindt.
  - Aantonen dat je aan de regels voldoet, informatieplichten
  - Privacy moet in de genen van je organisatie zitten

De IT-jurist

Privacyverordening
Nieuwe verplichtingen

- **Europese Privacyverordening**
  - Dataminimalisatie
  - Privacy by design / by default bij vernieuwing of wijziging informatiesysteem
  - Grotere bevoegdheden AP en andere handhavers, hogere boetes
  - Meldplicht datalekken
  - Aanstellen Functionaris voor de Gegevensbescherming
    - Overheden, stelselmatige observatie van betrokkenen en/of verwerking bijzondere persoonsgegevens (ras, gelood, geaardheid, gezondheid etc.)
  - Privacy Impact Assesment & Privacy Enhancing Technologies

De IT-jurist

Privacyverordening: bewerkersovereenkomst

- **Nadere regels over de bewerkersovereenkomst (art. 28 lid 3 Vo):**

  - Bewerker verwerkt uitsluitend op basis van schriftelijke instructies van de verantwoordelijke;
  - Bewerker moet vertrouwelijkheid waarborgen en beveiligingsverplichtingen verantwoordelijke in acht nemen en terzake voldoende garanties bieden;
  - Ook voor subbewerkers is toestemming nodig
  - Bewerker moet ondersteunen bij de afhandeling van een datalek
  - Bewerker moet verantwoordelijke zo nodig ondersteunen bij het uitvoeren van een ‘gegevensbeschermingseffectbeoordeling’ (PIA) en het vooraf raadplegen van de toezichthouder;
  - Bewerker moet audits en andere manieren om naleving van de wet aan te kunnen tonen mogelijk maken.

- **Eigen aansprakelijkheid van Bewerker wordt behoorlijk uitgebreid**
- **Bewerker loopt groot ondernemingsrisico als hij niet voldoet en niet afdoende garanties biedt**

De IT-jurist

Privacy Shield

- Safe Harbor: verdrag tussen VS en EU m.b.t. veilige uitwisseling van Europese persoonsgegevens
- Snowden
- Schrems arrest, Safe Harbor ongeldig
- Safe Harbor 2.0 door Europese Commissie: “Privacy Shield”
- Boetes voor gegevensuitwisseling op basis van de “waarborg” Safe Harbor worden inmiddels uitgedeeld

De IT-jurist

Privacy Shield

- Kritiek door Opinie Artikel 29 Werkgroep
  - Te ingewikkeld en onoverzichtelijk
  - Klachtprocedures te ingewikkeld en ineffectief
  - Rol Ombudsman onvoldoende gewaarborgd
  - Massasurveillance nog steeds niet uitgesloten
- Ook kritiek van Europese toezichthouder gegevensbescherming en Europees Parlement

De IT-jurist

Privacy Shield

- Standard Contractual Clauses
  - De vraag is of Amerikaanse partijen die willen tekenen
  - De vraag is of die niet ongeldig worden verklaard
  - Facebook gebruikt nu model clauses in plaats van Safe Harbor. Schrems: andere juridische waarborgen, maar lossen onderliggend probleem niet op. Ierse AP kijkt ernaar.

- Wordt vervolgd

De IT-jurist

www.it-jurist.nl

volg ons op @DeITjurist

@Andre_Kamps

@OordtJW