Duthler Associates
law, ICT & organisation

# Demonstrate compliance,

Privacy wetgeving, een business case voor de informatiebeveiliger

Drs. André J. Biesheuvel RE RA

6 december 2016

Duthler Associates
law, ICT & organisation

## Agenda

'15: Inleiding
- Wet meldplicht datalekken en andere wetten;
- Toezichtsarrangement; en
- Gevolgen bedrijfsvoering: bent u accountable?

'15: Business case voor wie? en uiteindelijk de informatiebeveiliger

'15: De opdracht:
gaat om meer dan vertrouwelijkheid; ISO 27001 is behulpzaam en wat is de toegevoegde waarde van de informatiebeveiliger?

Duthler Associates
law, ICT & organisation

# Wie zijn wij en met wie werken wij samen?

- **Juristen, adviseurs & auditors**
  Speerpunt: privacy en veiligheid
- **Partner:**
  drs. André J. Biesheuvel RE RA | Duthler Associates
- **Advocaat:**
  mr. dr. Anne-Wil Duthler| First Lawyers

Duthler Associates
law, ICT & organisation

# Wet Meldplicht datalekken

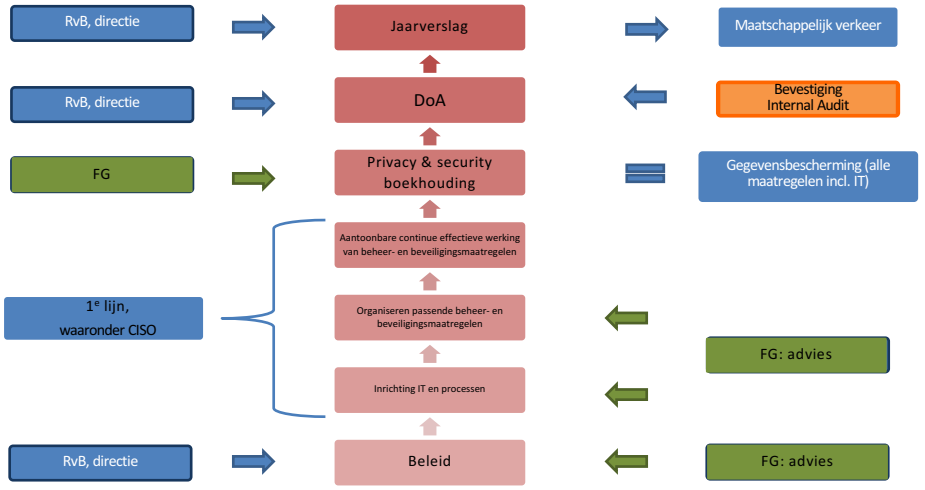

**Uit de speech van Butarelli van 26 mei 2016:**

I have been arguing that the biggest policy and legal innovation in the GDPR is the notion of accountability.

**That notion**, now transcribed into Article 24 of the new EU Regulation 2016/679, **requires controllers to comply and to demonstrate compliance with the new rules. The notion of accountability will expand soon outside the EU**. However as Chris Graham and others have said many times in the last few years the biggest practical innovation in the EU is the introduction of serious sanctioning powers. The possibility of fines in the EU of up to 4% of annual global revenue this is the provision which should make an impact in executive board rooms round the world. It should make an impact –but whether it will make an impact depends on many authorities in this conference. Taken together three factors create a potentially robust regime for safeguarding digital rights:

Accountability enhanced powers of independent authorities and several substantive articles requiring and prescribing cooperation between those authorities.

## Bent u accountable?




## Business case samenleving & betrokkene

- Samenleving, één informatie-eco-systeem in Eurozone
  - Neem de burgen serieus!
  - **Opportunity costs:**
    - Onverschilligheid / populisme: uiteenvallen van de Europese Unie (!)
    - Verschillen in productiviteit: verscheurt de Euro en uiteindelijk de Europese Unie
- Betrokkene (individu)
  - Burger krijgt controle eigen leven terug, digitale grondrechten worden serieus genomen
  - Ik heb het instrumentarium mijn rechten effectiever en kostenefficiënter uit te oefenen
  - EU concept richtlijn EP en Raad betreffende bepaalde aspecten van overeenkomsten voor de levering van digitale inhoud
  - **Kosten zijn voor de betrokkene nihil. Wat levert het op, voorbeelden: open calculatie en verlagen van de risicopremies!**

Duthler Associates
law, ICT & organisation

# Business case bedrijven en instellingen

- Noodzakelijke randvoorwaarden

  Neem klanten, burgers, patiënten het individuen serieus : ***persoonsgegevens mag u slechts onder voorwaarden gebruiken***.
  - Voorziet u in "**awareness raising and training of staff**" in de haarvaten van de organisatie?
  - Heeft u een adequate normenset (**legal policy framework – baseline – policy rules**)?
    Bent u "**accountable**"? En bent u in staat "**demonstrate compliance**"?
- Ja?, dan is er een business case
  - Afspraken maken in een netwerk van verantwoordelijk- en aansprakelijkheden
    **Operationele besparingen: meer dan 50%, zie #004*: waarom een Wbo?* en *besparingen contractbeheer***
  - Privacy & security accounting
    **Operationele besparingen: meer dan 20% - 60%, zie #006: *Avg, Risk & Compliance is dat genoeg?***
  - Accountability evidence based inregelen & auditability risk based vormgeven
    **Operationele besparingen: meer dan 20% - 40%, zie #005: *beheersen van de audit overkill***

Duthler Associates
law, ICT & organisation

# Business case informatiebeveiliger

- Noodzakelijke randvoorwaarden
  - Voldoende kennis en ervaring "**evidence based**" beschermen persoonsgegevens en informatieveiligheid
  - Sociale vaardigheden, multi-disciplinair en biedt FG comfort
  - Formuleer uw business case
- Business case, wat levert het op als u mij (IBer) inzet?
  - Kennispartner en liaison informatiebeveiliging in een organisatie overschrijdend netwerk van samenwerkende partners
    **Operationele besparingen: onontgonnen gebied, vergaande standaardisatie en optimalisatie mogelijk**
  - Privacy & security accounting technische informatie-infrastructuren
    **Besparen op operationele en auditkosten : stel op 50%**
  - Risk based minitoren en plannen op basis van een adequate normenset: LPFBPr en systematisch vastgelegd bewijs effectieve werking beheers- en beveiligingsmaatregelen
    **Operationele besparingen: voorkomen sanctie, maar belangrijker civiele zaak**

# Observaties

- Aanpassingen vraagstelling ∫(wetgeving;business)
  - Kunt u innoveren?: scope en reikwijdte, rollen en “demonstrate compliance”;
  - ISO 27001 vormt een orderdeel van privacy & security accounting; en
  - Wat draagt de IB bij aan ontlastend bewijs effectieve werking van beheers- en beveiligingsmaatregelen?
- IB financials: kwantificeren van de opportunity costs

  Realiseer wat u belooft
  - Aan wet- en regelgeving gerelateerde normenset en gemotiveerd volwassenheidsniveau;
  - Adequate producten die het gewenste bewijs in de organisatie kunnen genereren; en
  - Vastleggen van het bewijs en risk based monitoren effectieve werking beheersmaatregelen technische infrastructuur.

# Contactinformatie

Voor meer informatie kunt u contact opnemen met:

**Drs. André J. Biesheuvel RE RA**
Managing Partner
Mail: a.j.biesheuvel@duthler.nl
Frankenslag 137
2582 HH Den Haag
Tel: 070 392 22 09

**Mr. dr. Anne-Wil Duthler**
Advocaat / Partner
Mail: a.w.duthler@firstlawyers.nl
Frankenslag 137
2582 HH Den Haag
Tel: 070 306 00 33