DE CLERCQ

De Master spreekt… Privacywetgeving 2018 (AVG)

KNVI-bijeenkomst
SIG IT-Recht / SIG-IT Audit
Vrijdag 29 september 2017

KNVI
Koninklijke Nederlandse Vereniging van Informatieprofessionals

DECLERCQ

De Privacy Test

Wat is uw privacy IQ?

Surf naar de website kahoot.it om mee te doen!

Privacy

- Privacy terecht een veelbesproken thema
- Privacy bij herziening Grondwet in 1983 opgenomen als grondrecht
- Individu vandaag opgenomen in honderden tot duizenden bestanden (en datalekken doen zich veelvuldig voor!)

Wet– en regelgeving

- De belangrijkste regels vastgelegd in Wet bescherming persoonsgegevens (Wbp)
- Daarnaast schrijven andere wetten privacyregels voor (bijv. Wet algemene bepalingen Burgerservicenummer, Wet op de geneeskundige behandelingsovereenkomst)

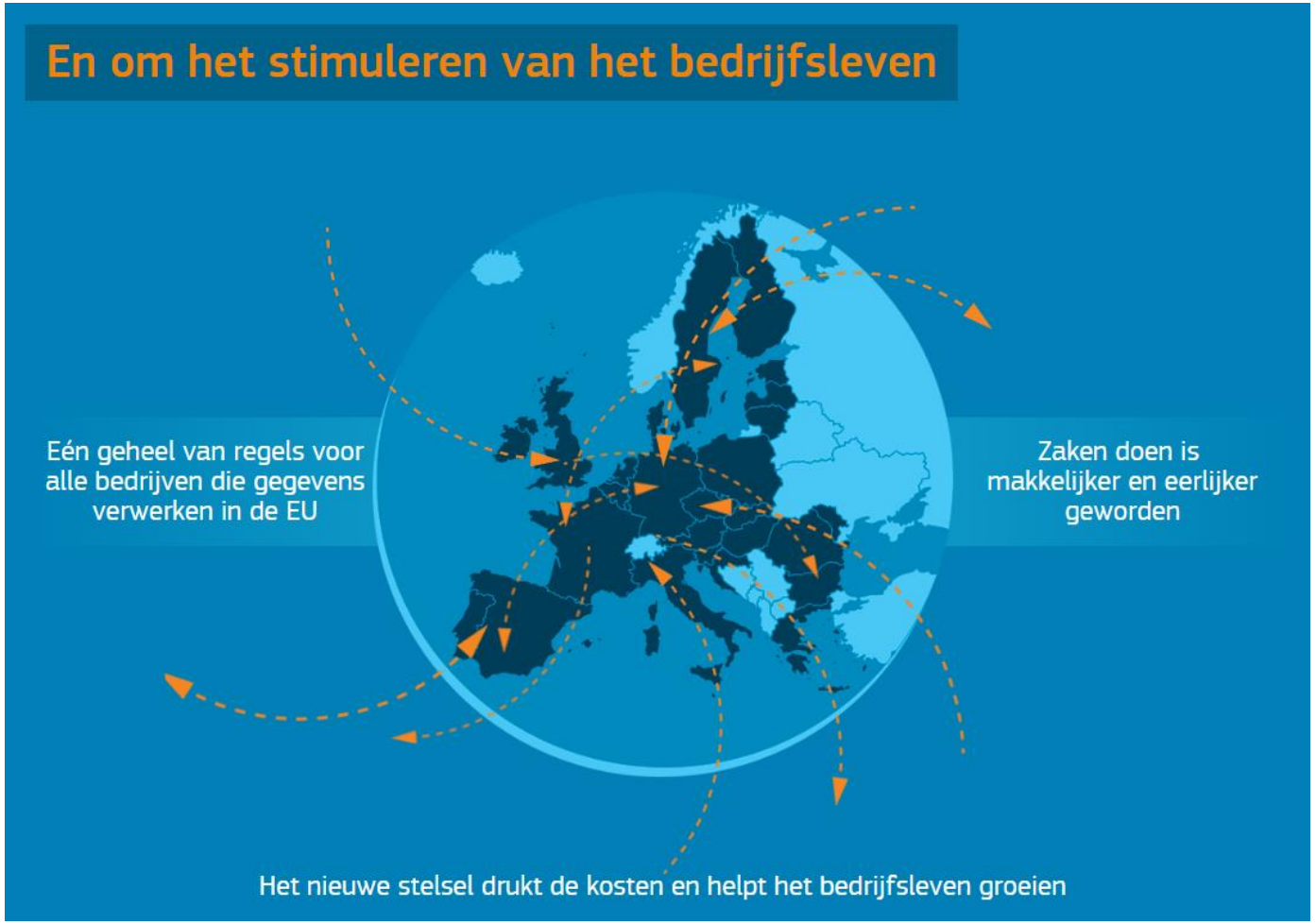
Algemene Verordening Gegevensbescherming

- Vanaf 25 mei 2018 geldt de Algemene Verordening Gegevensbescherming (AVG)
- De Wbp komt dan te vervallen: vanaf 25 mei 2018 is er één privacywet in de hele EU (in plaats van 28 nationale wetten)

Waarom worden de regels gewijzigd?

Bron: http://ec.europa.eu/justice/newsroom/data-protection/infographic/2017/index_nl.htm

Waarom worden de regels gewijzigd?



Bron: http://ec.europa.eu/justice/newsroom/data-protection/infographic/2017/index_nl.htm

Persoonsgegevens

- De privacyregelgeving is alleen van toepassing op de *verwerking* van *persoonsgegevens*

- Wat zijn “persoonsgegevens”?
  - Alle informatie over een geïdentificeerde persoon of een persoon die redelijkerwijs geïdentificeerd kan worden (“de betrokkene”)

Persoonsgegevens

Bron: http://ec.europa.eu/justice/newsroom/data-protection/infographic/2017/index_nl.htm

Verwerken

- Wanneer is sprake van het “verwerken” van persoonsgegevens?

- Vrijwel iedere handeling, zoals bijvoorbeeld:
  - Verzamelen
  - Vastleggen
  - Ordenen
  - Structureren
  - Opslaan
  - Bijwerken
  - Wijzigen
  - Opvragen
  - Raadplegen
  - Gebruiken
  - Verstrekken
  - Doorzenden
  - Verspreiden
  - Ter beschikking stellen
  - Combineren
  - Wissen

De wet bepaalt wat wel en niet is toegestaan

- Een organisatie mag alleen persoonsgegevens verwerken als dat noodzakelijk is voor een bepaald doel
- Een organisatie mag de persoonsgegevens vervolgens niet gebruiken voor een ander doel
- Persoonsgegevens mogen alleen worden verwerkt voor zover de gegevens ‘ter zake dienend’ en ‘niet bovenmatig zijn’.
- Persoonsgegevens mogen niet langer worden bewaard dan noodzakelijk is

Beveiligingsmaatregelen

- Organisaties moeten passende technische en organisatorische beveiligingsmaatregelen treffen

- Wat is in een concreet geval “passend”? Dit is afhankelijk van:
  - De stand van de techniek
  - De kosten van de beveiligingsmaatregelen
  - De risico’s die gepaard gaan met de verwerking
  - De aard van de verwerkte gegevens

Informatieplicht

- Organisaties moeten de betrokkene informeren over de verwerking

- De informatieplicht omvat in ieder geval:
  - Wie verwerkt de gegevens (de identiteit van de verantwoordelijke)
  - Welke gegevens worden verwerkt
  - Voor welk doel worden de gegevens verwerkt
  - Nadere informatie zoals:
    - Of de gegevens worden gedeeld met derde partijen
    - Of de gegevens worden doorgegeven naar partijen in niet-EU landen

Internationaal gegevensverkeer

- Binnen de EU: toegestaan
- Buiten de EU: in principe verboden, tenzij:
  - het derde land (volgens de Europese Commissie) een passend beschermingsniveau waarborgt
  - de EU-modelcontracten (ongewijzigd) worden gebruikt
  - de betrokkene hiervoor expliciet toestemming heeft gegeven
- Let op:
  - Het verbod geldt ook binnen concernverband!
  - Verbod geldt zowel voor de verwerkingsverantwoordelijke als verwerker
  - Brexit

Landen met een passend beschermingsniveau

- Andorra

- Argentinië

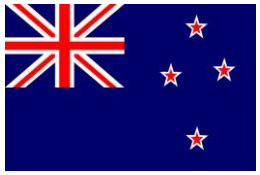
- Canada

- Guernsey

- Israel

- Isle of Man

- Jersey



- Nieuw Zeeland

- Uruguay

- Zwitserland

Landen met een passend beschermingsniveau

Opvallende afwezige: de Verenigde Staten

- Safe Harbour agreement is gesneuveld bij het Europees Hof
- Inmiddels vervangen door het Privacy Shield
- Veel kritiek, ook vanuit de Autoriteit Persoonsgegevens

- Let op: de verwachting is dat het Privacy Shield (uiteindelijk) geen stand zal houden

Privacy Shield Framework

Meldplicht

- **Iedere verwerking dient te worden gemeld bij Autoriteit Persoonsgegevens**
  - **Melding voorafgaand aan de aanvang van de verwerking**
  - **Geen verplichting indien verwerking is opgenomen in het Vrijstellingsbesluit (veel voorkomende verwerkingen zoals personeelsadministratie, salarisadministratie, krantenabonnementen en ledenadministraties)**

Rechten van betrokkenen

- Organisaties moeten ervoor zorgen dat betrokkenen hun rechten kunnen uitoefenen (zoals recht op inzage, verbetering, aanvulling, verwijdering of afscherming, etc.)

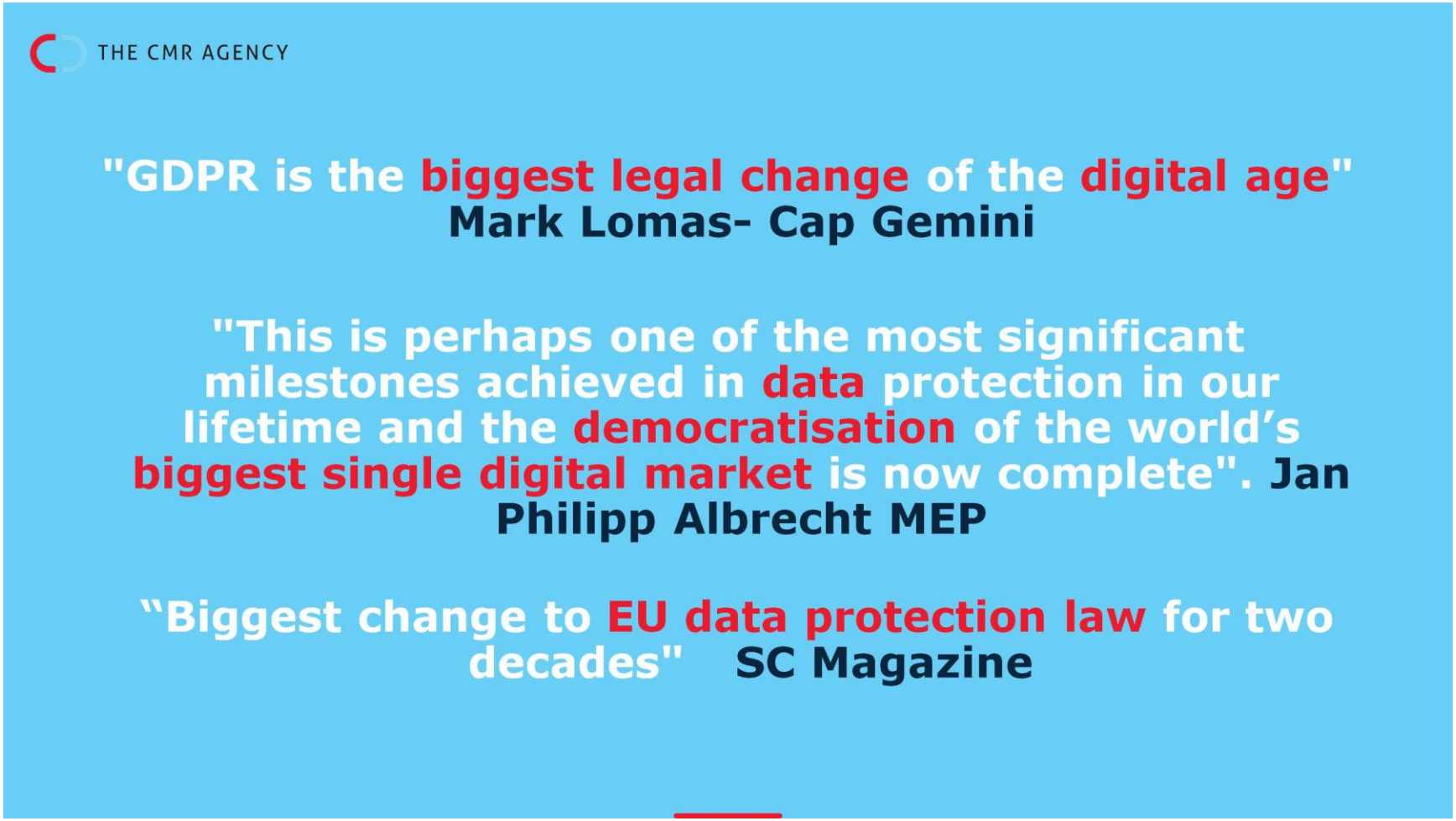
- Organisaties moeten er rekening mee houden dat zij (tijdig) aan verzoeken van betrokkenen kunnen voldoen:
  - Technisch mogelijk?
  - Gestroomlijnd proces voor het afhandelen van verzoeken?
  - Afspraken met bewerkers?

Bewerkers?

- Verplichting tot sluiten bewerkersovereenkomst

- Afspraken over:
  - welke beveiligingsmaatregelen de bewerker moet treffen
  - hoe de verantwoordelijke toezicht gaat (en mag) houden op de naleving
  - hoe en wanneer datalekken moeten worden gemeld
  - of de bewerker onderaannemers (‘subbewerkers’) mag gebruiken

Wat verandert er vanaf 25 mei 2018?



http://thecmragency.com/2017/03/13/voorbereidende-informatie-gdpravg-avg-seminar/

Registratieplicht

- Verwerkingen hoeven niet meer vooraf te worden gemeld bij Autoriteit Persoonsgegevens
- In plaats daarvan moeten zowel verwerkers als verwerkingsverantwoordelijken een verwerkingsregister bijhouden, met daarin:
  - De doelen van de verwerking
  - Van wie persoonsgegevens worden verwerkt
  - Welke persoonsgegevens worden verwerkt
  - Met welke derde partijen de gegevens worden gedeeld
  - Wat de bewaartermijn van de gegevens is
  - Welke beveiligingsmaatregelen zijn getroffen
  - Of de gegevens worden verzonden naar het buitenland, en zo ja, naar welk land

Uitzondering registratieplicht

- Organisaties met minder dan 250 werknemers hoeven geen register bij te houden, tenzij:
  - Het waarschijnlijk is dat de verwerking een risico inhoudt van de rechten en vrijheden van de betrokkenen;
  - De verwerking niet incidenteel is; of
  - Er bijzondere persoonsgegevens of strafrechtelijke gegevens worden verwerkt.

Uitbreiding rechten van betrokkenen

- Vanaf 25 mei 2018 krijgen betrokkenen meer rechten, onder meer:
- Recht op gegevenswissing
  - Op verzoek van de betrokkene moeten gegevens wordt gewist als die niet meer relevant zijn
  - Derden aan wie de gegevens zijn verstrekt moeten worden geïnformeerd over het verzoek
- Recht op overdraagbaarheid van gegevens (dataportabiliteit)
  - Kopie van de persoonsgegevens in een elektronisch en bruikbaar formaat

Functionaris voor de gegevensbescherming

- Is verplicht (zowel voor verwerker als verwerkingsverantwoordelijke) indien:
  - Organisatie een overheidsinstantie of overheidsorgaan is
  - Organisatie hoofdzakelijk en op grote schaal regelmatig en stelselmatig betrokkenen observeert
  - Organisatie op grote schaal bijzondere persoonsgegevens of strafrechtelijke gegevens verwerkt

- Let op: er wordt een groot tekort aan functionarissen voorzien!

Gegevensbeschermingseffectbeoordeling (PIA)

- In veel gevallen verplichting PIA uit te voeren. In ieder geval in het geval van:
  - systematische en uitgebreide beoordeling van persoonlijke aspecten van natuurlijke personen, gebaseerd op een geautomatiseerde verwerking (incl. profilering) en op grond waarvan besluiten met rechtsgevolgen worden genomen of die op andere wijze significante gevolgen heeft voor een natuurlijk persoon;
  - Grootschalige verwerking van bijzondere of strafrechtelijke persoonsgegevens;
  - Stelselmatig en grootschalig monitoren van openbaar toegankelijke ruimten.
- De Europese toezichthouders zullen een lijst publiceren voor welke verwerkingen in ieder geval een PIA moet worden gedaan

Privacy by Design & Privacy by Default

- Organisaties zullen verplicht zijn gegevens te beschermen middels *privacy by design* (ontwerp) en *privacy by default* (standaardinstellingen)
- Al in de ontwerpfase van een applicatie of ICT-systemen zal er dus rekening mee moeten worden gehouden dat voldoende technische waarborgen worden ingebouwd!

Uitbreiding wettelijke verplichtingen voor verwerkers

- Bijhouden van verwerkingsregister
- Afsluiten van een verwerkersovereenkomst (gezamenlijke verantwoordelijkheid met verwerkingsverantwoordelijke)
- Na afloop van de dienstverlening alle persoonsgegevens verwijderen of aan de verwerkingsverantwoordelijke retourneren
- Geen subverwerkers inschakelen zonder voorafgaande toestemming van de verwerkingsverantwoordelijke
- Overeenkomsten met verwerkers sluiten, met daarin dezelfde verplichtingen als in de verwerkersovereenkomst met de verwerkingsverantwoordelijke

Uitbreiding wettelijke verplichtingen voor verwerkers (vervolg)

- Voor zover mogelijk, technische en organisatorische maatregelen treffen om de verwerkingsverantwoordelijke bij te staan bij het nakomen van de rechten van betrokkenen

- Voor zover mogelijk, de verwerkingsverantwoordelijke bij te staan bij het voldoen aan de verplichtingen omtrent beveiliging, meldplicht datalekken en PIA

Uitbreiding wettelijke verplichtingen voor verwerkers (vervolg)

- Meewerken aan audits en controle van de verwerkingsverantwoordelijke
- Verwerkingsverantwoordelijke onmiddellijk in kennis stellen indien een instructie een inbreuk op de AVG oplevert
- De verwerkingsverantwoordelijke ‘zonder vertraging’ te informeren van een inbreuk in verband met persoonsgegevens

DECLERCQ

Boetes en aansprakelijkheid

Boete

Wbp

- Maximaal € 820.000,- of 10% van de jaarlijkse wereldwijde omzet
- Verplichtingen zijn ingedeeld in drie categorieën, een hogere categorie betekent een hogere boete
- Hoogste categorie:
  - Verwerking bijzondere persoonsgegevens
  - Verwerking BSN
- Autoriteit Persoonsgegevens moet een bindende aanwijzing geven, voordat een boete wordt opgelegd, tenzij sprake is van opzet of ernstige nalatigheid

Boete

Wbp

- Boete-verhogende omstandigheden:
  - Recidive
  - Tegenwerken of belemmeren onderzoek

- Boete-verlagende omstandigheden:
  - Vergaande medewerking
  - Zelfstandige beëindiging overtreding
  - Zelfstandige schadeloosstelling betrokkenen

Boete

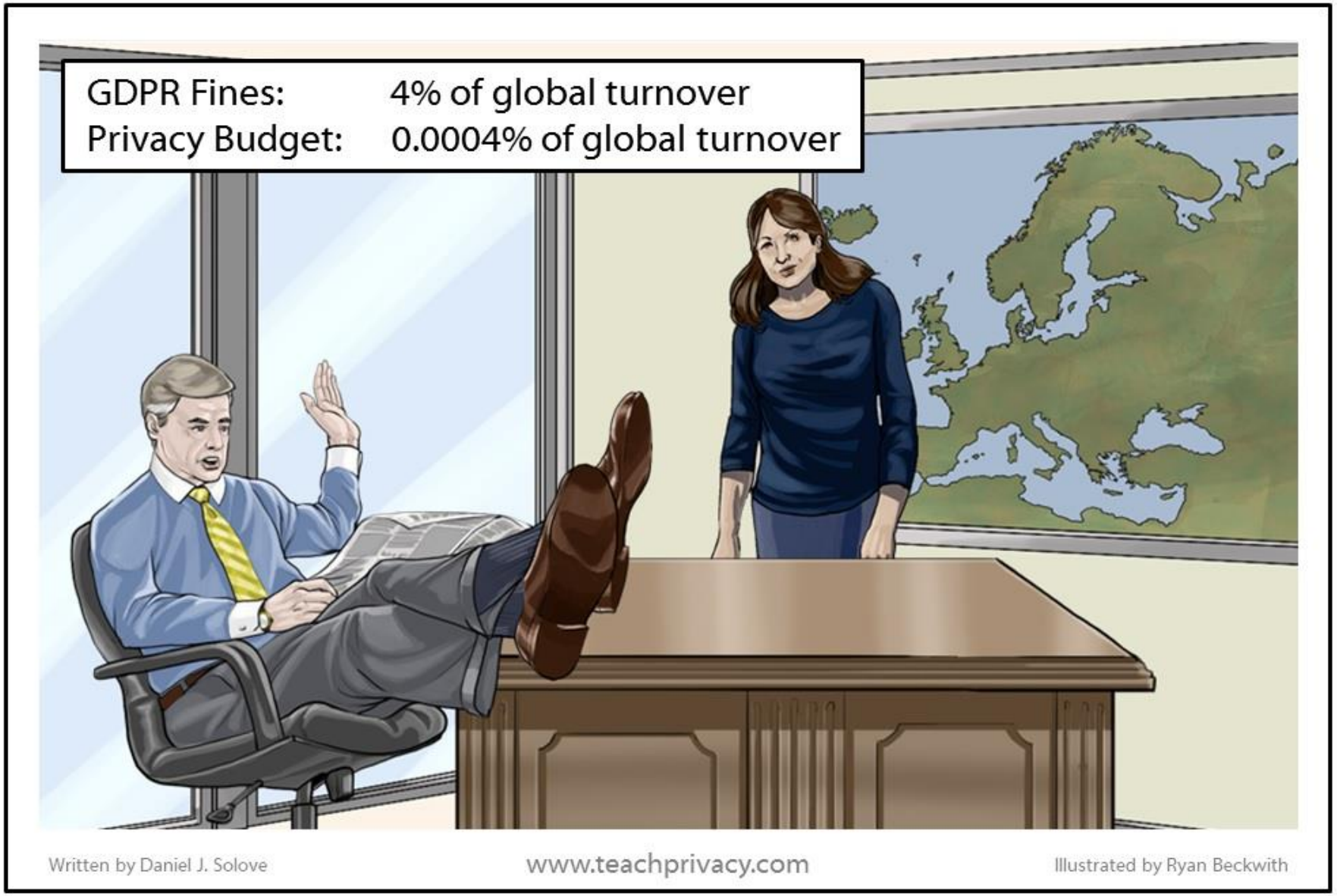
AVG

- Autoriteit Persoonsgegevens is niet langer verplicht eerst een bindende aanwijzing te geven
- Bij de afweging of een boete wordt opgelegd, wordt rekening gehouden met:
  - Opzet of nalatigheid
  - Eerdere inbreuken
  - Of de inbreuk zelfstandig is gemeld
  - Of de inbreuk betrekking heeft op bijzondere persoonsgegevens
  - In hoeverre is samengewerkt met de Autoriteit Persoonsgegevens om de gevolgen te beperken
  - Andere relevante omstandigheden, zoals met de inbreuk gemaakte winst

Boete

AVG

- Voor overtreding van het merendeel van de verplichtingen maximaal € 10.000.000,- (of 2% van de jaarlijkse wereldwijde omzet), zoals:
  - Privacy by design
  - Register van verwerkingen
  - Passende beveiliging
- Voor de belangrijkste verplichtingen maximaal € 20.000.000,- (of 4% van de jaarlijkse wereldwijde omzet), zoals:
  - Rechten van betrokkenen
  - Verwerking van bijzondere persoonsgegevens
  - Verplichtingen bij doorgifte naar landen buiten de EU


GDPR Fines: 4% of global turnover
Privacy Budget: 0.0004% of global turnover
Written by Daniel J. Solove
www.teachprivacy.com
Illustrated by Ryan Beckwith

Boete

Bestuurdersaansprakelijkheid

- Autoriteit Persoonsgegevens kan – ook nu al – een boete opleggen aan een onderneming, of aan de persoon die feitelijk leiding heeft gegeven aan de verboden gedraging

- Dit kan de bestuurder zijn (bestuurdersaansprakelijkheid) maar ook een ander persoon binnen de organisatie

Wat moeten organisaties nu concreet doen?

- ✓ Medewerkers trainen en zorgen voor een privacybewuste organisatie
- ✓ Nagaan welke persoonsgegevens worden verwerkt (data inventarisatie)
- ✓ Voorbereiden op de registratieplicht
- ✓ Opstellen van een privacybeleid met inrichting evaluatiecyclus, met onder meer:
  - ✓ *Privacy by Design/Default* bij nieuwe producten of diensten
  - ✓ PIA bij bestaande en nieuwe producten of diensten
- ✓ Updaten van bewerkersovereenkomsten
  - ✓ Indien (nog) niet aanwezig, zo snel mogelijk afsluiten!
  - ✓ Protocol meldplicht datalekken (en actueel houden)
- ✓ Functionaris voor gegevensbescherming aannemen of opleiden?
- ✓ De AVG gaat uit van accountability: u moet kunnen aantonen dat u aan de wet voldoet. Alle acties, overwegingen en keuzes moeten worden gedocumenteerd!

Vragen?

Natascha van Duuren
Voorzitter SIG IT-Recht

n.vanduuren@declercq.com
071 581 53 56