MORRISON
FOERSTER

EVALUATIE - HANDHAVING VAN DE AVG

Vereniging Privacy Recht

Alex van der Wolk

2 december 2019

Handhaving in vogelvlucht

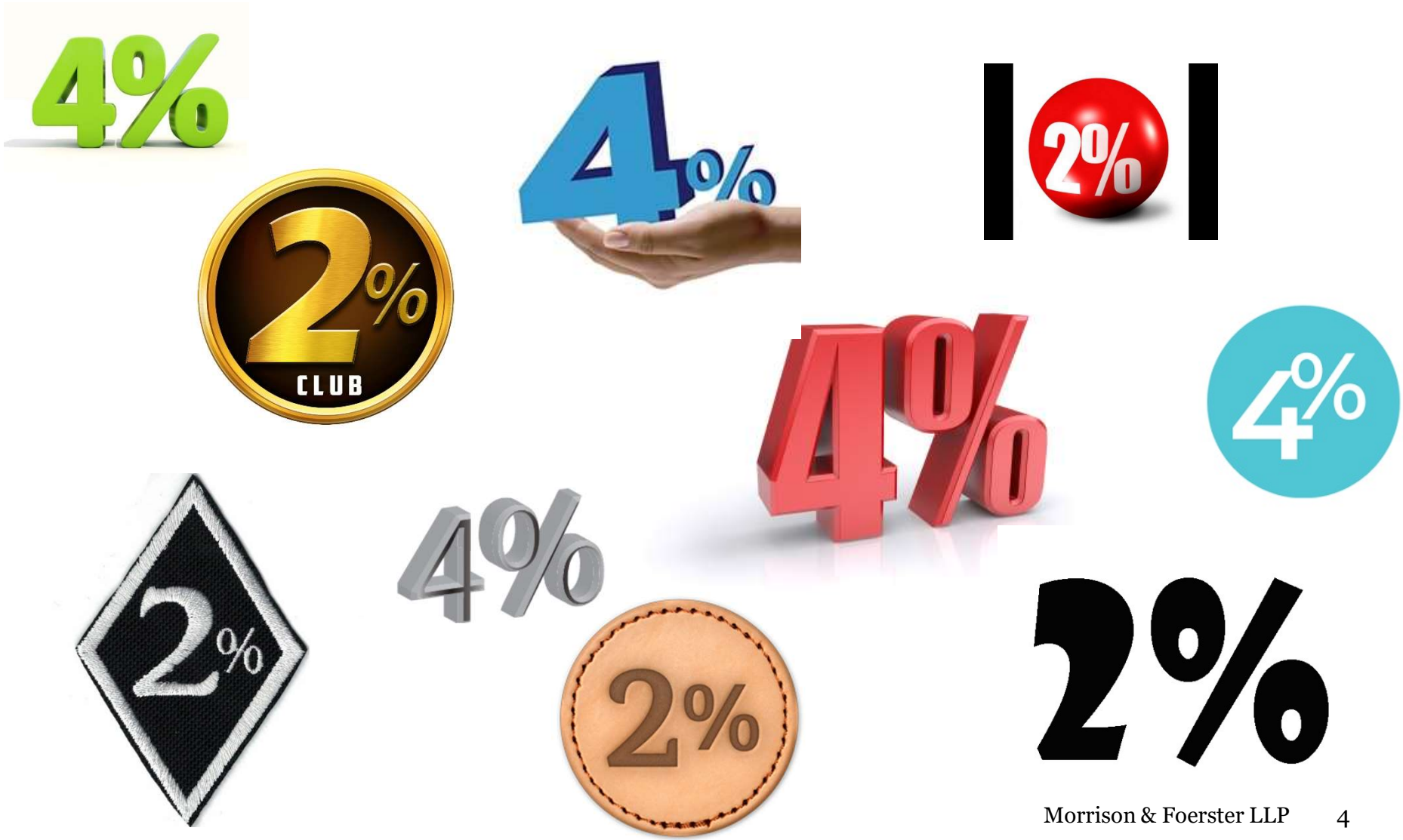
Wat hebben we *niet* gezien?

1. Dawn raids

Alhoewel…

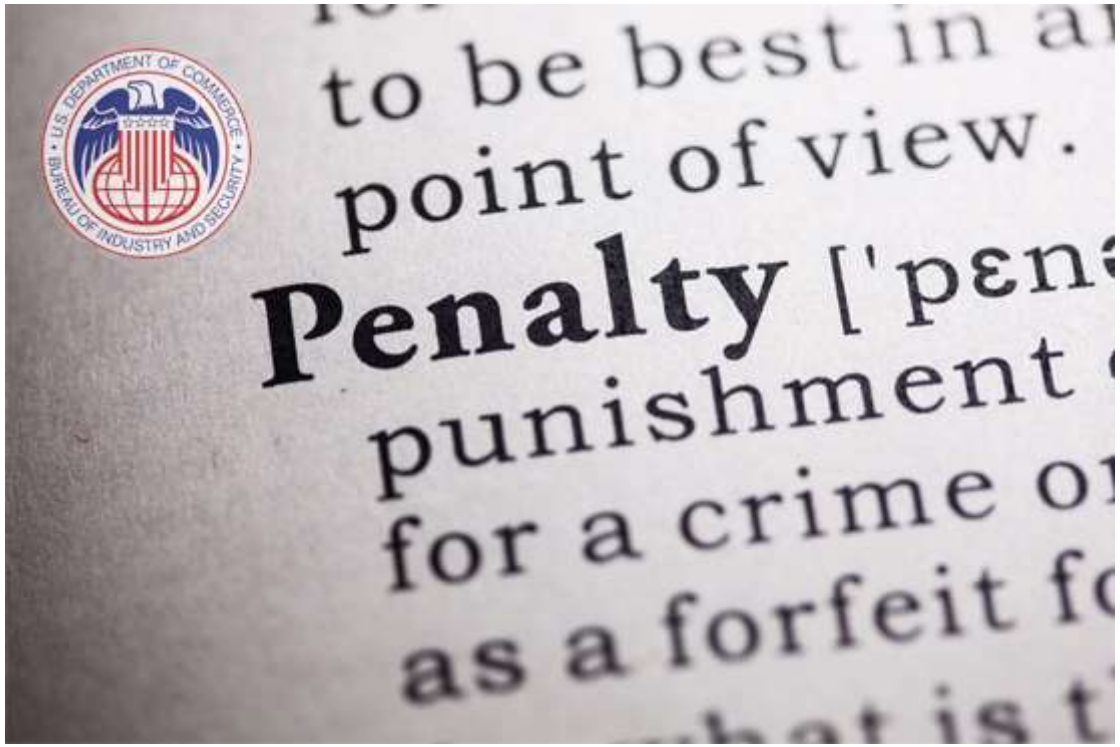

ico.
Information Commissioner's Office
Enforcement
ico.
Information Commissioner's Office
Enforcement

2. Maximum boetes 2% / 4%



Alhoewel…

3. Uniform boetebeleid

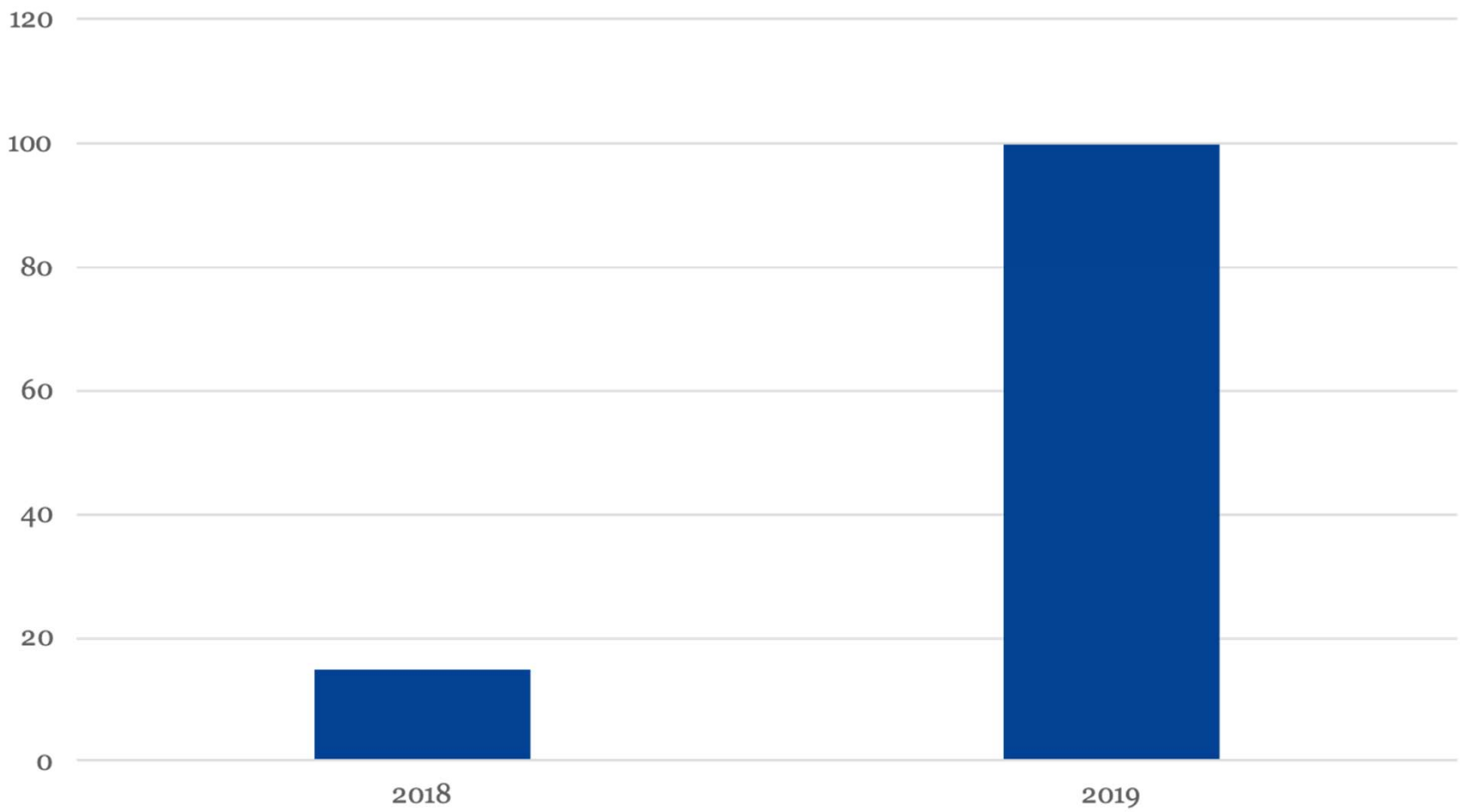


Handhaving in vogelvlucht

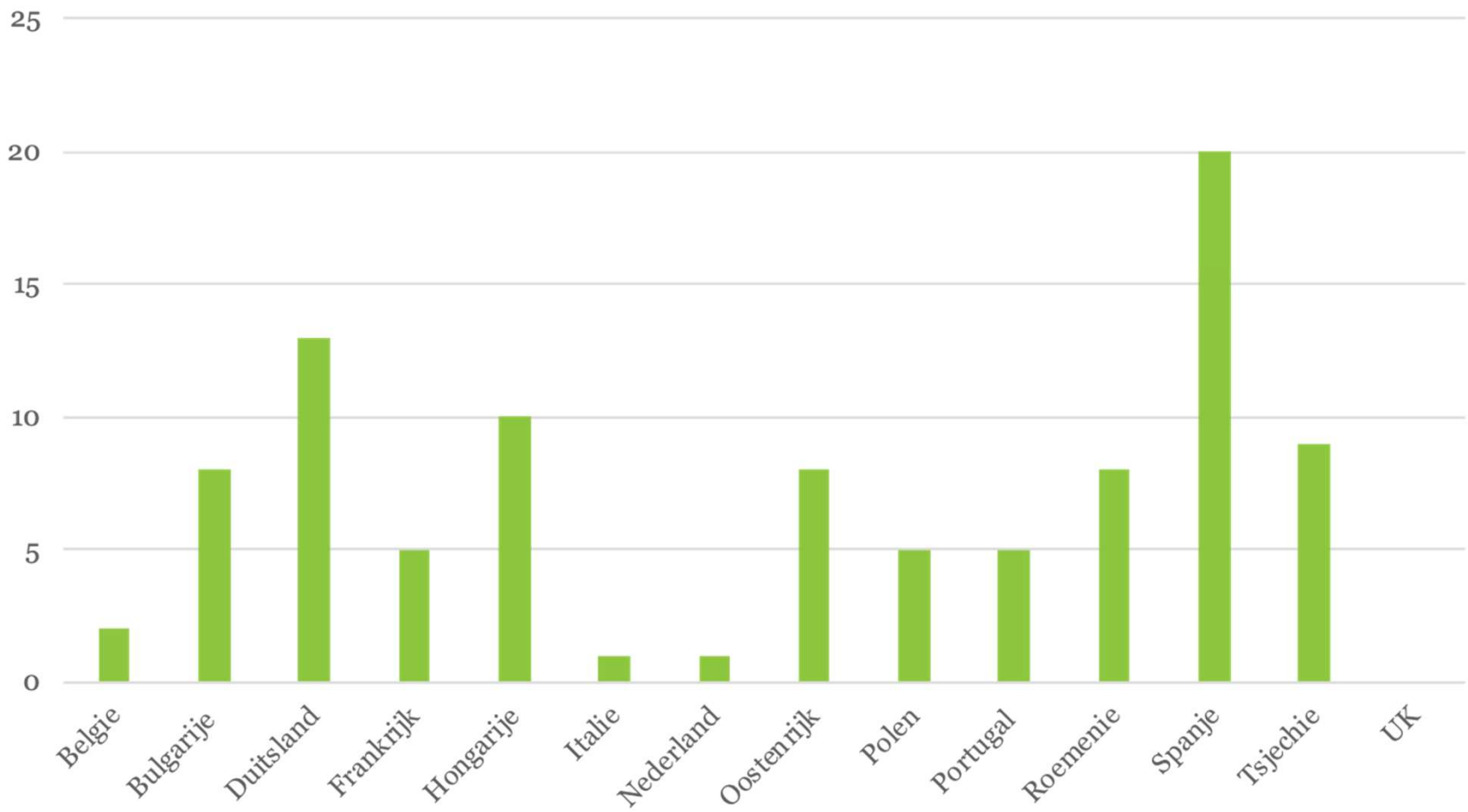
Wat hebben we *wel* gezien?

Handhavings acties

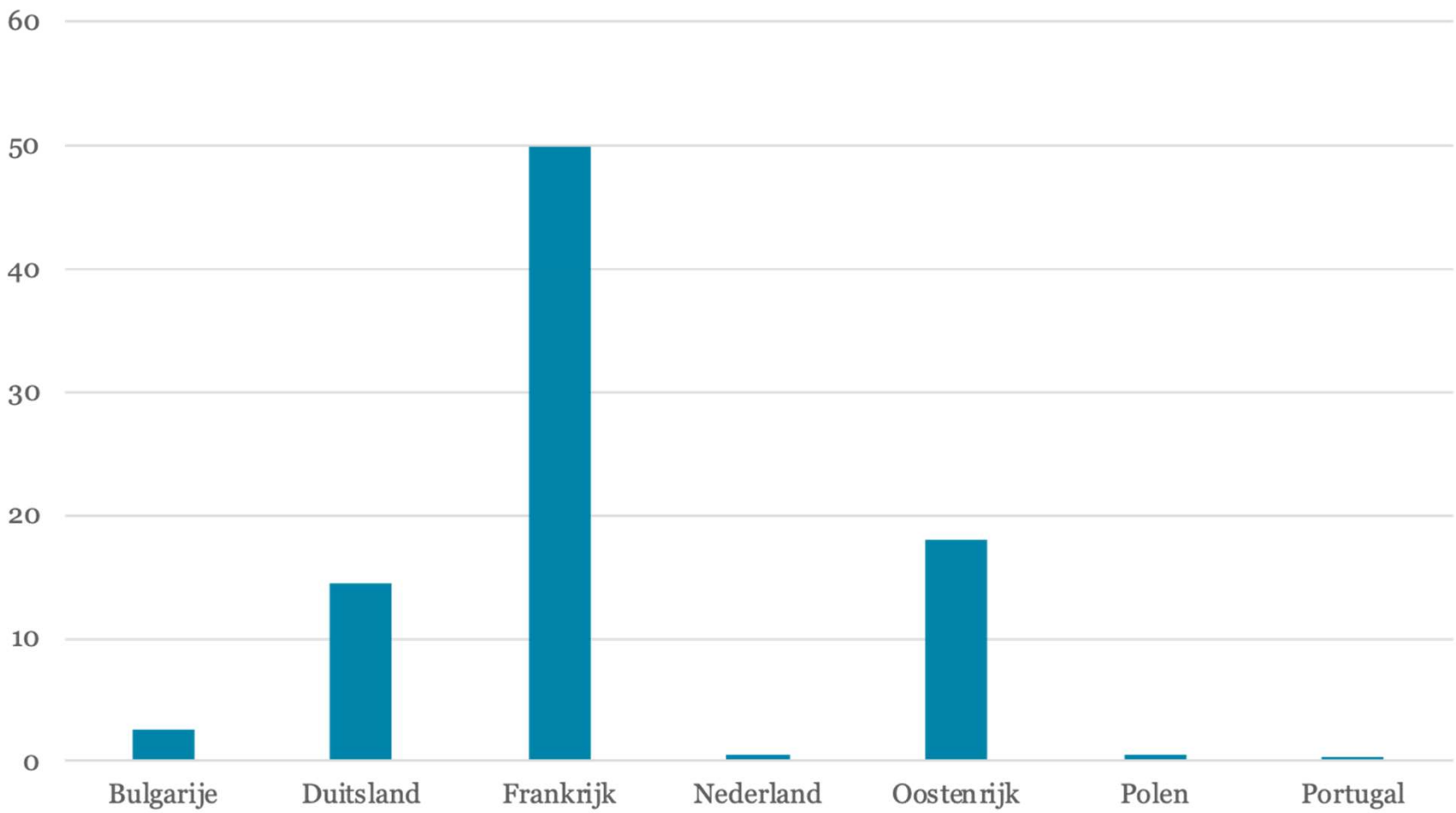
Aantal handhavings acties



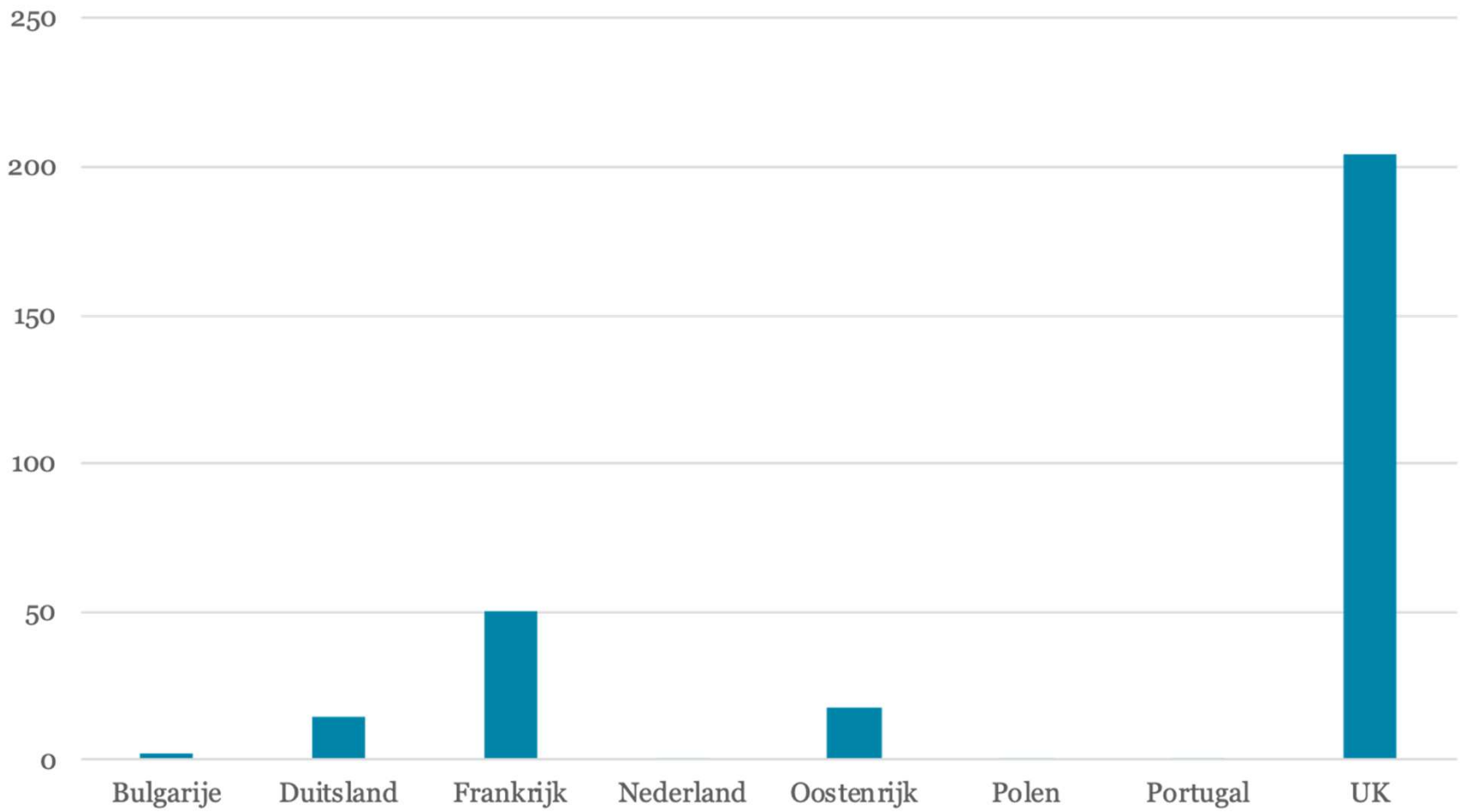
handhavings acties per land



Hoogte van boetes (mio)



Hoogte van boetes (mio)



Hoogte van boetes

- 4 boetes van > € 1 mio
  - FR, AU, DU, BU
- ~20 boetes van > € 100.000
  - o.a. PO, FR, DU, NL, BU, PU, SP, NO, DK, GR, LE, RO
- ~ 40 boetes van > € 10.000
  - o.a. HU, DU, LI, SP, AU, IT, SL, PO, HU, FR, SW
- Laagste boetes in categorie van enkele honderden euro
  - E.g. Oostenrijk: € 300 voor ongeoorloofd gebruik van dashcam

Handhavingsacties

- Meerendeel van handhavingsacties (>30) ging over beveiligingslekken c.q. beveiligingstekortkomingen
  - UK: British Airways (€204 mio) en Marriott (€110 mio) - beide beveiligingslekken
  - Bulgarije: NRA (€2,6mio) – hacking attack
  - Polen: Morele.net (€644K) – beveiligingstekortkoming
  - Nederland: Haga Ziekenhuis (€460K) – beveiligingstekortkoming
  - Frankrijk: Sergic (€400K)
  - Portugal: Barreiro Montijo (€400K)
- Opvallend: slechts enkelen (ca. 5) gingen over te laat melden van beveiligingslek

CNIL/Google

- Hoogste boete tot nu toe
  - Betrof onderzoek door CNIL n.a.v. klacht van *None of Your Business* en *La Quadrature du Net*
  - Android platform

- Tekortkomingen:
  - *Transparantie*: informatie te veel verspreid over verschillende documenten. Bovendien, de verwerkingen waren *massive* and *intrusive* vanwege hoog volume van verschillende bronnen waar Google informatie uit verkrijgt
  - *Toestemming*: onvoldoende geïnformeerd (mede vanwege veelvoud aan diensten) en niet-specifiek niet-ondubbelzinnig. Veel opties waren standaard aangevinkt.

UODO (Polen) / ClickQuickNow

- Beperken recht van intrekken van toestemming
  - Bedrijf vereiste reden van intrekking
  - Suggereerde op webpagina dat intrekking voltooid was, waarna gebruiker werd doorgeleid
- DPA:
  - Overtreding van recht op verwijdering (omdat toestemming niet effectief kon worden ingetrokken)
  - Overtreding van accountability (Art. 24) om uitoefening rechten van individuen te kunnen voldoen
  - Overtreding van principes van rechtmatigheid, fairness en transparantie.
- Boete: € 47.000

Berlin DPA / Deutsche Wohnen

- Boete voor overtreding van Privacy by Design principe

- Meer specifiek: geen adequate retention policy
  - Geen verwijdering van data
  - Geen review van noodzaak om data te behouden
  - In sommige gevallen was data aanwezig waar geen enkele noodzaak voor was, waaronder loonstroken, belastingformulieren, zorgverzekerings informatie

- Boete: € 14,5 miljoen
  - DPA woog mee dat Deutsche Wohnen opzettelijk het gewraakte systeem in gebruik had genomen, ondanks al in 2017 hiervoor gewaarschuwd te zijn geweest.
  - DPA heeft nieuwe boeteleidsregels toegepast

Oostenrijk DPA / AU Post

- Overtreding vanwege verwerking van bijzondere persoonsgegevens
  - Oostenrijkse Post maakte geïnformeerde gissingen van politieke voorkeuren
  - Het feit dat dit een 'berekende waarschijnlijkheid' deed niet af aan verwerking van bijzondere persoonsgegevens
- Boete
  - Niet onderbouwd hoe tot € 18 mio komt
  - Interessant: € 800 schadevergoeding voor individuele eiser voor civiele rechtbank
    - Potentiele groep eisers: 2,2 miljoen individuen.

AP / Haga Ziekenhuis

- Medische gegevens van Bekende Nederlander in ziekenhuis opgezocht door medewerkers
- Melding door Haga aan AP
- Beveiliging in zorgsector: NEN 7510 en 7513
  - O.a. twee-factor authenticatie
  - Het bijhouden van log-files

- Haga had slechts enkelvoudige authenticatie en beoordeelde de logfiles niet regelmatig
- Bovendien: zelfs na ontdekking (jan 2018) werden NEN normen niet toegepast

- In aanvulling van boete € 460.000, ook last onder dwangsom

ICO / British Airways

- Boete volgende op cyber incident
  - Vanaf juni 2018 werd internet verkeer afgevangen en doorgeleid naar een valse website
  - BA meldde het lek in september 2018 aan ICO
- Boete voor onvoldoende beveiliging
- Interessant:
  - Boete nog niet definitief; betreft enkel aankondiging
  - ICO heeft aankondiging gedaan in reactie op regulatory disclosure door BA aandeelhouders (ivm beurs disclosures) – geeft spanningsveld aan tussen verplichting van beursgenoteerde bedrijven om materiele events kenbaar te maken.

Boetebeleidsregels Nederland

- Neemt als startpunt de aard van de overtreding

- Elk artikel is ingedeeld in categorie I, II, III of IV, bijv.:
  - I: Art. 26, 30, 37(7)
  - II: Art. 25, 28, 37
  - III: Art. 27(3), 31, 33, 34
  - IV: Art. 9, 22

Categorie	Startpunt	Bandbreedte
I	€ 100.000	€ 0 – 200.000
II	€ 310.000	€ 120.000 – 500.000
III	€ 525.000	€ 300.000 – 750.000
IV	€ 725.000	€ 450.000 – 1.000.000

Boetebeleidsregels - Duitsland

- Neemt als startpunt de omzet van de onderneming

STEP 1

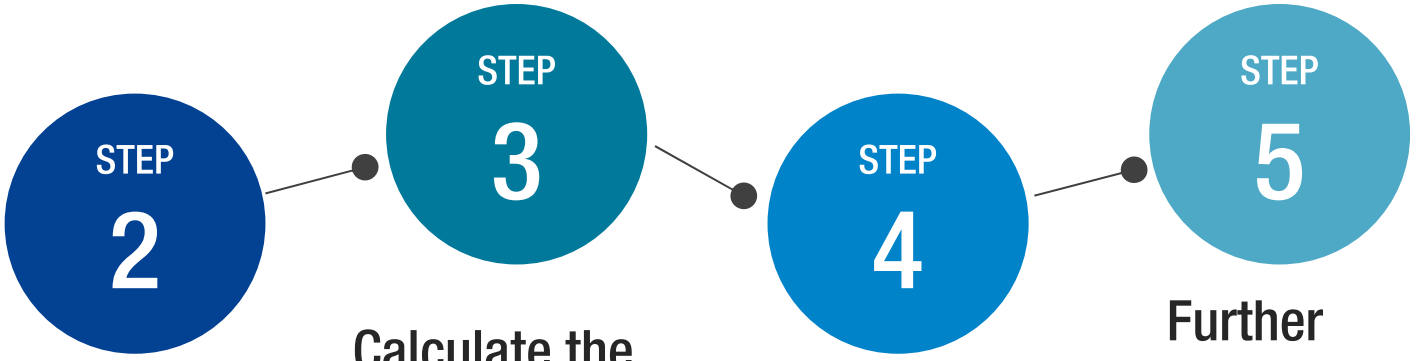
Classify company by size

By global annual turnover.

Micro-Enterprises < € 2mio	Small Enterprises € 2-10 mio	Medium-sized Enterprises € 10-50 mio	Large Enterprises > € 50 mio
Subgroup 1	Subgroup 1	Subgroup 1	Subgroup 1
Subgroup 2	Subgroup 2	Subgroup 2	Subgroup 2
Subgroup 3	Subgroup 3	Subgroup 3	Subgroup 3
		Subgroup 4	Subgroup 4
		Subgroup 5	Subgroup 5
		Subgroup 6	Subgroup 6
		Subgroup 7	Subgroup 7

Boetebeleidsregels - Duitsland

- Aan de hand van de classificatie vinden de volgende stappen plaats



Determine the average turnover

Determine each subgroup's average annual turnover.

Calculate the "daily rate"

By dividing the average turnover (step 2) of a company's subgroup by 360.

Determine the severity of offence

Multiply the daily rate by a factor between 1 and 12, depending on the severity of the offence (Art. 83 (2) GDPR).

Further considerations

Determine the relevance of any other criteria under Article 83(2) GDPR.

Hoe pakt dat dan uit?

- Voorbeeld: overtreding van beveilingsverplichting, art. 32

- Nederland
  - Valt in categorie II: €120.000 – 500.000 / startpunt: € 310.000
  - Verzwarende factoren: aard van betrokkenen (e.g. patiënten), structurele voortduring van overtreding, hoge mate van vertrouwensschending, niet regelmatig controleren van beveiliging, nalatige aard van de inbreuk.
  - Eindboete: € 460.000

- Duitsland
  - Onderneming heeft jaaromzet van ca. € 9 miljoen
    - Is daarmee een “small enterprise”
    - Valt in categorie B.III: gem. omzet € 8,75 miljoen / dagtarief: € 24,306
    - Art. 32 = formele overtreding (Art. 83(4))
    - Ernstige overtreding (factor 6) = € 145.836
  - Bij omzet van € 150 mio: boete van € 2,5 mio

Uniformiteit?

- Gepubliceerde boetebeleidsregels alleen voor Nederland, Duitsland en Portugal

- Boetes in overige handhavingsacties zijn ongemotiveerd
  - Wordt aangegeven dat Art. 83(2) in acht is genomen
  - En dat uiteindelijke boete binnen maximum van AVG blijft
  - Maar geen indicatie van startpunt
  - Geen indicatie van hoe verzwarende en verlichtende factoren zijn gewogen
  - Geen indicatie hoe cumulatie van overtredingen bijdragen aan totale boete

- De afwezigheid van beleidsregels leidt tot onvoorspelbaarheid en dissonantie van boetes

- Vgl. Mededingsrecht waar EC beleidsregels op EU niveau heeft vastgesteld

One Stop Shop

- Duidelijk dat OSS geen ‘one-off’ beoordeling is
  - Gaat om verwerking, niet om organisatie als geheel

- CNIL: “OSS niet van toepassing, omdat Ierse vestiging geen beslissings bevoegdheid had over verwerkingsactiviteiten”

- CNIL heeft intentie om zaak te behandelen gecommuniceerd via ”EU informatie exchange system”, maar niemand protesteerde (in welk geval EDPB zaak had moeten behandelen).

- Klopt het dat “beslissingsbevoegdheid” de crux is voor OSS? Of gaat het enkel om ”centrale administratie”, zonder dat deze ook doel en middelen in voorkomend geval moet vaststellen?

What's next?

MORRISON
FOERSTER