

@zwnne

# General Problems Faced With Respect To the Application of DP Directive 95/46/EC and Some Suggestions to Resolve These

Prof. mr. G-J. (Gerrit-Jan) ZWENNE | Istanbul

25 April 2017



Universiteit  
Leiden



# prof. dr. G-J. (Gerrit-Jan) ZWENNE

- law professor at Leiden University, with a strong focus on privacy and data protection
- lawyer and partner at Brinkhof, Tech lawfirm in Amsterdam

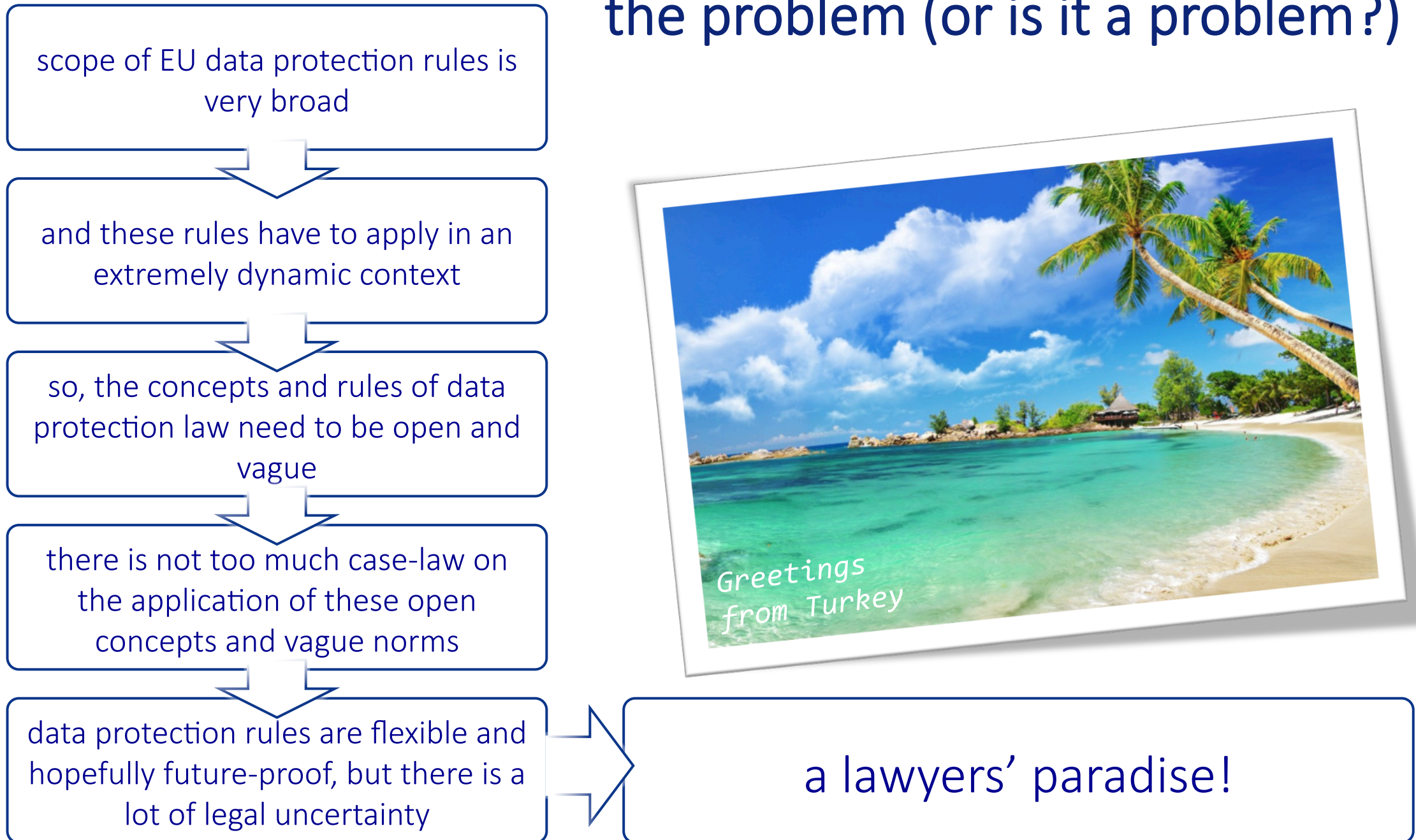


*"He offers vast experience in data protection issues. Sources respect his "academic standpoint" on legal developments in the area, and he has published numerous materials related to his field"*



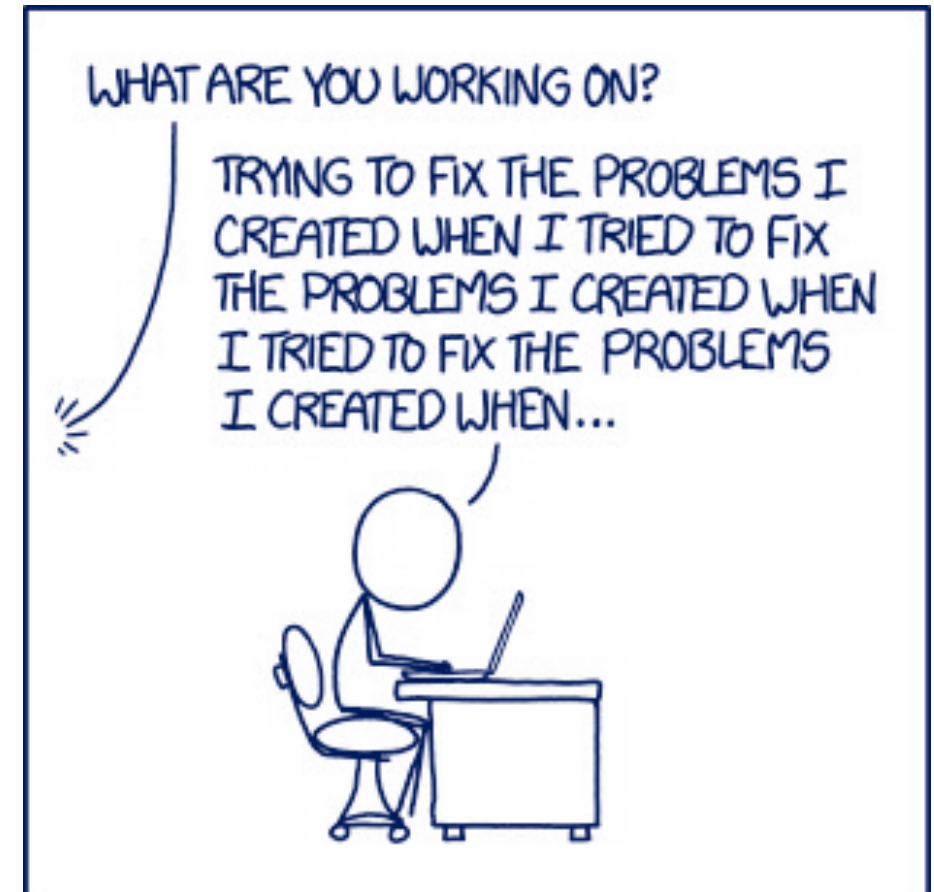
*"Data privacy expert Gerrit-Jan Zwenne joined Brinkhof from Bird & Bird LLP in February 2016. The practice's key strengths include multi-jurisdictional outsourcing and advising household-name clients"*

# the problem (or is it a problem?)



# some of the most common problems <sup>in my experience...</sup>

1. are IP-addresses and other online **identifiers** always personal data?
2. what to do with **special data** (health and ethnic data, criminal records, etc.)..?
3. data subject **access requests**: what should be provided, and what not?
4. questions on consent and '**cookie-consent**' particularly for mobile devices



# what are personal data?

Art. 4(2) GDPR &  
Art. 2(a) 95/46/EC

‘personal data’ means any  
information relating to an  
*identified* or *identifiable*  
natural person (‘data subject’)

is *singling-out* sufficient?

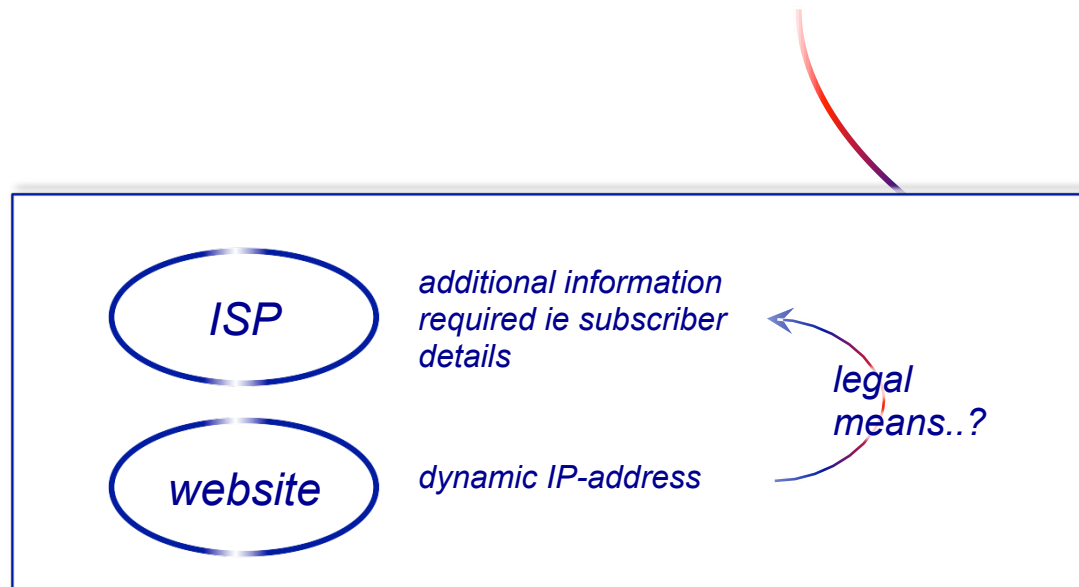
The million-dollar question: are *IP-  
addresses* or *MAC-addresses* (and  
the like) personal data?





*a dynamic IP address registered by an online media services provider when a person accesses a website that the provider makes accessible to the public, constitutes personal data within the meaning of that provision, in relation to that provider, where the latter has the legal means which enable it to identify the data subject with additional data which the internet service provider has about that person.*

CJEU 19 October 2016  
C-582/14 (Breyer)



So, an IP-address or MAC-address qualifies as personal data, to the extent that one has the legal means to obtain all additional information necessary to determine the identity of the user of that address

# 'special data'

*possibly also issues with respect to rules for profiling and automated decision-making*

*in case of legal consequences or similar material effects on data subject*

*only allowed*

- *for the execution of a contract with data subject*
- *on the basis of an act that provides adequate safeguards*
- *with explicit data subject consent*

## data types

- health data
- ethnic data
- criminal records
- religion
- political party
- trade union membership
- biometric ID-data
- genetic data
- social security number

## rules

- processing only by **specific controllers** for **specific purposes**, etc. or
- with data subject **explicit consent**, or
- evidently **made public** by data subject, or
- **specific law** or **DPA-decision** that provides adequate safeguards
- etc.

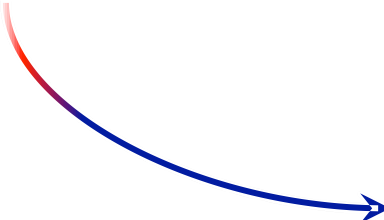
## issues

- interpretation (e.g. photo's, date of birth, etc.)
- set-up of fraud detection & prevention systems
- wearables at work
- monitoring eye-movements in trucks
- photo copy of passports, etc.

# data subject access requests

- what should be provided: a copy of the original file(s) or an overview of the data?
- a right to obtain personal data that the controller actually has – *not* a right to have data made at request(!)

CJEU 17 July 2014  
C-141/12 and C-372/12  
(IND vs YS et al)



Typically, there is a lot of case-law on data subject access requests, and related issues, e.g. material scope of the law



# problems with consent

- in employer-employee relationships
- differentiated consent
- no provision of service, unless data subject consents to the processing of data that is not needed for the provision of that service

*"[Consent is considered not likely freely given] where there is a clear imbalance between the data subject and the controller" [recital 43 GDPR]*

*"Consent can only be valid if the data subject is able to exercise a real choice, and there is no risk of deception, intimidation, coercion or significant negative consequences if he/she does not consent." [Art. 29 WP Opinion on Consent of 13 July 2011]*

*"Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case." [recital 43 GDPR]*

*When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract. [Art. 6(4) GDPR]*

*cf. recital 43 GDPR (?)*

# cookie consent

## rules:

cookies may only be used

- if the user is fully informed about *inter alia* the purposes for which the data will be used, and
- if the user has consented

*incl. similar technology, e.g. device fingerprinting, pixels, javascript etc.*

*consent button, continued use of the website, swiping on a mobile device*

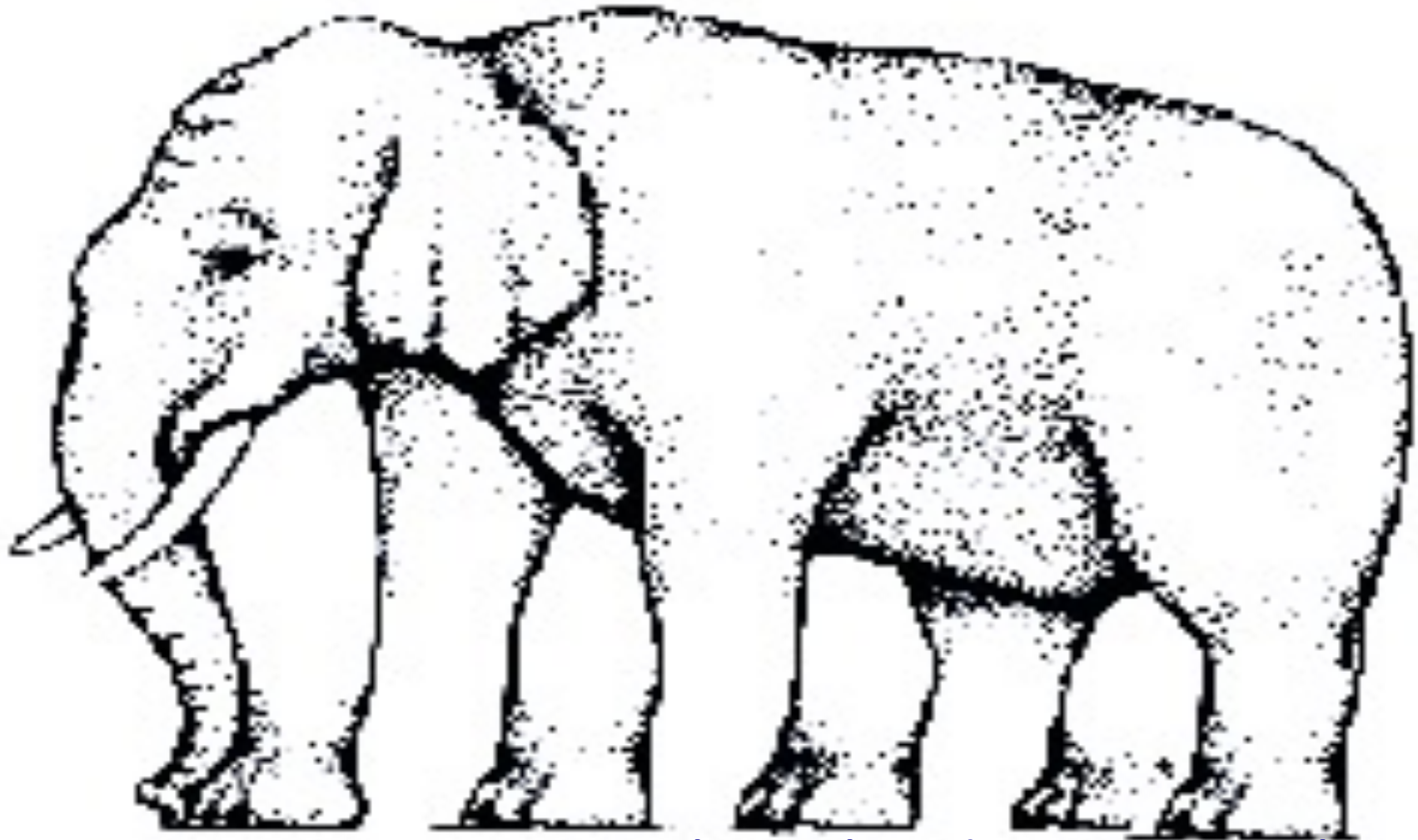
*what about **cookiewalls**...*

*practical problem: how to provide all information on small screens..?*

*solution: layered information notices (banner, cookie policy, cookie table)*

## exemptions:

- functional or technical cookies, ie cookies needed to provide the (web)service
- non-privacy intrusive first party analytic cookies



[g.j.zwenne@law.leidenuniv.nl](mailto:g.j.zwenne@law.leidenuniv.nl)