

PRIVACY AND EU DATA PROTECTION

Seminar III. and IV.

Main principles. Lawful processing. Purpose specification and purpose limitation.

prof. dr. Gerrit-Jan Zwenne



September 09th, 2020

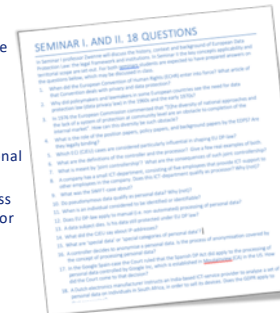
1

QUIZ

Question 18 preparation assignment questions

A Dutch electronics manufacturer instructs an India-based ICT-service provider to analyse a set of personal data on individuals in South Africa, in order to sell its devices. Does the GDPR apply to that processing?

- No, because no goods or service are offered to data subjects in the EU and/or there is no monitoring of their behaviour (as far as their behaviour takes place within the Union)
- No, the individuals are not in the EU, nor are the residents or citizens of member states, and consequently they are not protected by the GDPR
- Yes, as the GDPR applies to the processing of personal data in the context of the activities of an establishment of a controller in the Union, regardless of whether the processing takes place in the Union or not.



2

QUIZ

Question 12 preparation assignment questions

Does EU DP-law apply to manual (i.e. non-automated) processing of personal data?

- No, the GDPR applies only to the processing of personal data wholly or partly by automated means
- Yes, the GDPR also applies to processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system
- No, because such non-automated processing falls outside the scope of Union law
- Yes, because the non-automated processing does not affect the free movement of personal data within the Union



3

QUIZ

Is an IP-address personal data?

- It could be if the entity that has access to that IP-address has the legal means which enable it to identify the data subject with additional data which the internet service provider has about that person
- Yes, because an IP-address allows the identification, directly or indirectly, of the internet-user
- No, because an IP-address identifies a device connected to the internet (e.g. a tablet, computer or a mobile phone), but not necessarily the user of that device
- No, but a so-called MAC-address is.

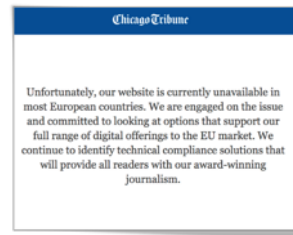


4

QUIZ

Why would this US newspaper show this pop-up to EU-based internet-users that want to access an article on its website

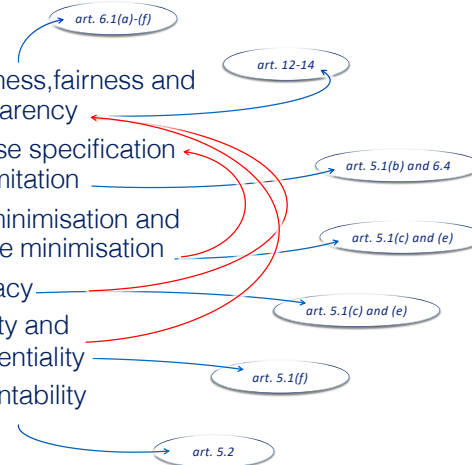
- The newspaper does not have an establishment in the EU and consequently it is not allowed to provide services to EU-residents
- The US does not provide an adequate level of data protection and therefore it cannot transfer personal data to member states
- The newspaper wants to demonstrate it does not offer services to data subjects in the EU. Consequently, the GDPR does not apply



5

principles

- lawfulness, fairness and transparency
- purpose specification and limitation
- data minimisation and storage minimisation
- accuracy
- integrity and confidentiality
- accountability



6

Recital 39
Art. 5.1(a) GDPR

'fair relationship between
controller and data subject'

"lawfulness, fairness and transparency" means
personal data is processed lawfully, fairly and in a
transparent manner in relation to the data
subject

eg. a privacy statement, intranet
employees' handbook, QR-code,
icons, etc.

7

Art. 5.1(d) GDPR

"accuracy" means personal data is
accurate and, where necessary, kept up to
date; every reasonable step must be taken
to ensure that personal data that are
inaccurate, having regard to the purposes
for which they are processed, are erased or
rectified without delay

8

Art. 5.2 GDPR

“accountability” processed under the responsibility and liability of the controller, who shall ensure and be able to demonstrate the compliance with the provisions of this Regulation

9


QUIZ

Which article(s) of the GDPR contain(s) the the data accuracy principle and the accountability principle?

A. Art. 5.1(a) and Art. 5.2
 B. Art. 5.1(d) and Art. 5.1(f)
 C. Art. 5.1(e) and Art. 5.(f)
 D. Art. 5.1(d) and 5.2

Which provisions in the GDPR set specific rules for processing so-called special data?

A. Art. 10
 B. Art. 9
 C. Recital 51
 D. Art. 6.4(c)

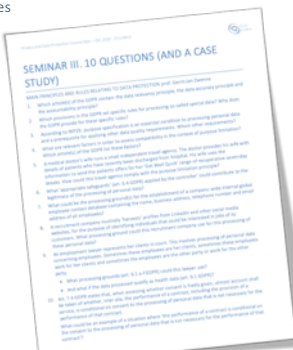


10

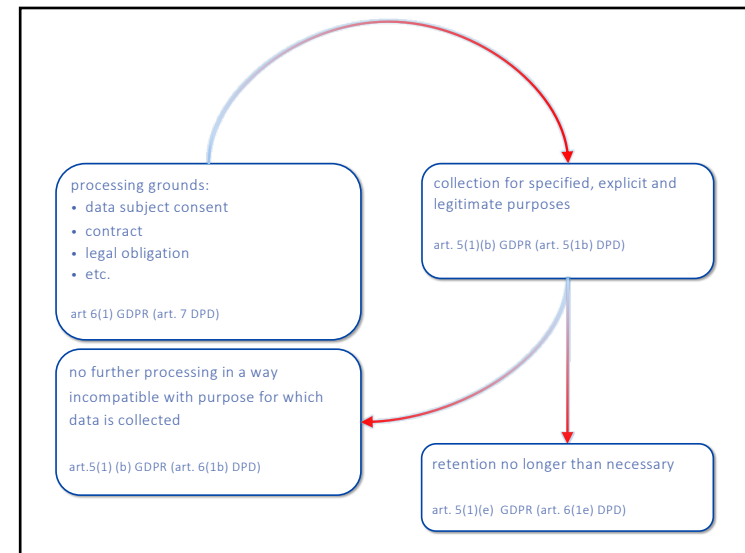
QUIZ

What are relevant factors to be used in order to assess compatibility in the context of purpose limitation?

A. the link between the purposes for which the personal data have been collected and the purposes of the intended further processing
 B. the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller
 C. the nature of the personal data, in particular whether special categories of personal data are processed
 D. the possible consequences of the intended further processing for data subjects
 E. existence of appropriate safeguards, which may include encryption or pseudonymisation
 F. All of the above



11



12

Art.6 GDPR

processing grounds (or basis for processing)

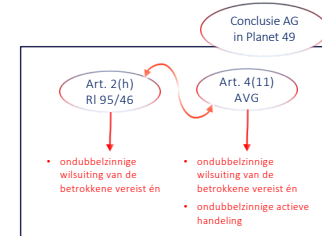
- data subject consent
- performance of a contract
- compliance with a legal obligation
- vital interest of the data subject
- public authority
- legitimate interest of controller or third parties to whom the data are provided

13

definition

Art. 4 (11) GDPR

any freely given, specific, informed and **unambiguous indication** of the data subject's wishes by which he or she, by a statement or by a **clear affirmative action**, signifies agreement to the processing of personal data relating to him or her



14

Art. 7 GDPR

conditions for consent

- burden of proof
- written declaration which also concerns another matter
- withdrawal of consent
- purpose limitation

consent must be presented clearly distinguishable in its appearance from this other matter

15

(32) Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.

not implied...

browser settings

consent should cover all purposes – but should consent be granular...?

not disruptive..

16

(42) Where processing is based on the data subject's consent, the controller should be able to demonstrate that the data subject has given consent to the processing operation. In particular in the context of a written declaration on another matter, safeguards should ensure that the data subject is aware of the fact that and the extent to which consent is given. In accordance with Council Directive 93/13/EEC (10) a declaration of consent pre-formulated by the controller should be provided in an intelligible and easily accessible form, using clear and plain language and it should not contain unfair terms. For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended. Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.

burden of proof

data subjects' awareness

clear and plain language

what constitutes detriment...?

17

(43) In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation. 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, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance.

asymmetry

seems much stricter than art. 7.4 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

18

(43) Consent is presumed not to be freely given if [...] the performance of a service, is dependent on the consent despite such consent not being necessary for such performance.

Article 7
4. 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.

19



AG Spuznar Opinion Planet49, par. 91

71. [T]he recitals of Regulation 2016/679 are particularly illuminating. Because I shall make extensive reference to the recitals, I feel compelled to recall that they obviously do not have any independent legal value, but that the Court frequently resorts to them in interpreting provisions of an EU legal act. In the EU legal order they are descriptive and not prescriptive in nature. Indeed, the question of their legal value does not normally arise for the simple reason that, typically, the recitals are reflected in the legal provisions of a directive. Good legislative practice by the political institutions of the EU tends to aim at a situation in which the recitals provide a useful background to the provisions of a legal text.

20

freely given...

In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a **clear imbalance** between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation

- *municipality vis-à-vis citizen*
- *drivers license agency vis-à-vis motorist*
- *employer vis-a-vis employee*
- *student vis-a-vis university*
- *etc.*

21

without detriment....

(42) Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent **without detriment**.



The Dutch data protection authority, the Autoriteit Persoonsgegevens, **announced** cookie walls are not compliant with the EU General Data Protection Regulation, TechCrunch reports. The AP issued guidance on the topic after it received complaints from internet users who were not allowed to go on a website after they refused to accept tracking cookies. The DPA said it has informed a number of the organizations in the complaints to stop the practice. "Cookie walls are non-compliant with the principles of consent of the GDPR," an AP spokesperson said. "Which means that any party with a cookie wall on their website has to be compliant ASAP, whether or not we will check that in a couple of months, which we certainly will do."

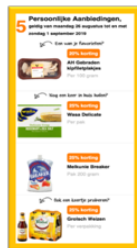
22

without detriment....

A supermarket asks for your consent to send you their weekly newsletter with substantial personal discounts.

You can withdraw your consent, but if you do so, you will no longer get these substantial personal discounts.

Is this consent valid in terms of the GDPR? **Can you withdraw your consent without detriment?**



23

granularity...

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 [...]



☐ I consent to the processing of my data for

- providing you our services
- informing you about our services
- informing you about our other services
- product development

I consent to the processing of my data for

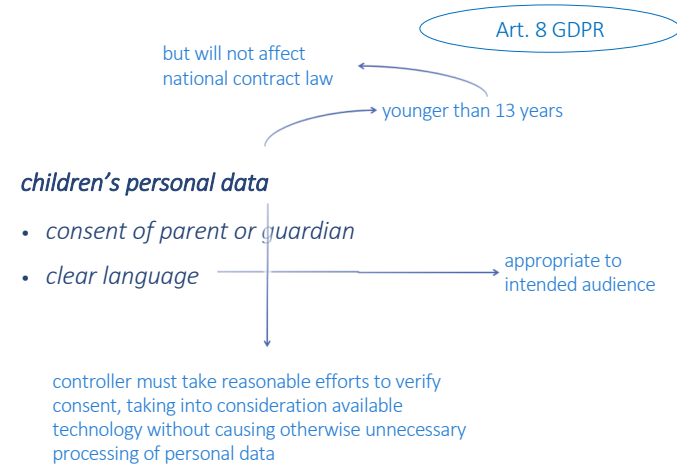
- ☐ providing you our services
- ☐ informing you about our services
- ☐ informing you about our other services
- ☐ product development

24



**PLEASE DO NOT TICK
THE BOX IF YOU DO
NOT WANT TO RECEIVE
OUR DAILY OFFERS IN
YOUR INBOX**

25



26



won't somebody
please think of the
children!?

27

vital interests



28

legitimate interest...

- has controller a legitimate interest?
- is the processing necessary for that interest?
- what is the impact on the data subjects interests, rights or freedoms, and to what extent is that proportionate?

the balance between the processing's effects on the interest of the controller on the one hand and the impact on the data subjects' interests

proportionality & subsidiarity

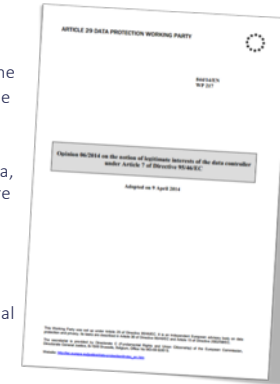
there is no alternative for the processing that will have less impact on the data subjects' interests

29

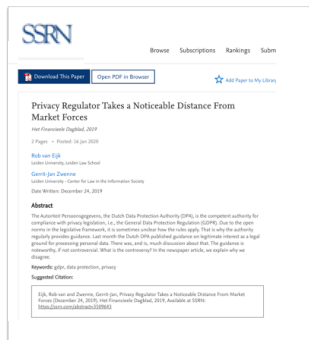
legitimate interest...

factors to consider when carrying out the balancing test :

- nature and source of the legitimate interest and whether the data processing is necessary for the exercise of a fundamental right, is otherwise in the public interest, or benefits from recognition in the community concerned;
- impact on the data subject and their reasonable expectations about what will happen to their data, as well as the nature of the data and how they are processed;
- additional safeguards which could limit undue impact on the data subject, such as data minimisation, privacy-enhancing technologies; increased transparency, general and unconditional right to opt-out, and data portability



30



Dutch Data Protection Authority Offers Its Take on 'Legitimate Interest' Data Processing Authority

By Oda Kagan on November 4, 2019

POSTED IN GENERAL PRIVACY & DATA SECURITY NEWS & DEVELOPMENTS

The Dutch DPA has issued guidance on the use of "legitimate interest" as a legal basis for processing data under GDPR.

Key takeaways on what constitutes "legitimate":

- The interest needs to be pursuant to a written or unwritten legal principle.
- Merely serving the interests of society or pure commercial interests, profit maximization, following the behavior of employees or the (buying) behavior of (potential) customers, etc. is not legitimate interest.
- This position seems not to be in line with previously expressed positions in the EU.
- For example, per the United Kingdom Information Commissioner's Office, individual interests in broader societal benefits may still be legitimate.
- The Article 29 Working Party in its opinion WP217 recognized legitimate interest as applying to certain types of marketing activities.



31

AG Bobek 19 December 2018, Case C-40/17 (Fashion ID)

122. Directive 95/46 does not define or enumerate 'legitimate interests'.

That notion appears to be rather elastic and open-ended. There is no type of interest that is excluded per se, as long of course as they are themselves legal.



32

three-step-process

1. *is the interest legitimate?*

2. *is processing necessary for that legitimate interest*

3. *are the privacy interest not disproportionately affected by the processing*

33

QUIZ

Question 8 preparation
assignment questions

A recruitment company routinely 'harvests' profiles from LinkedIn and other social media websites, for the purpose of identifying individuals that could be interested in jobs of its customers. What processing ground could this recruitment company use for this processing of these personal data?

- A. data subject consent (art. 6.1(a) GDPR)
- B. performance of a contract (art. 6.1(b) GDPR)
- C. general interest task (art. 6.1(e) GDPR)
- D. legitimate interest (art. 6.1(f) GDPR)
- E. All of the above



34

QUIZ

Question 9 preparation
assignment questions

An employment lawyer represents her clients in court. This involves processing of personal data concerning employees. Sometimes these employees are her clients, sometimes these employees work for her clients and sometimes the employees are the other party or work for the other party.

What processing grounds (art. 6.1 a-f GDPR) could this lawyer use?

- A. data subject consent (art. 6.1(a) GDPR)
- B. legal obligation (art. 6.1(c) GDPR)
- C. vital interests (art. 6.1(d) GDPR)
- D. legitimate interest (art. 6.1(f) GDPR)



35

Recital 39
Art. 5(1)(b) GDPR

“purpose specification” and “purpose limitation”
means personal data collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes

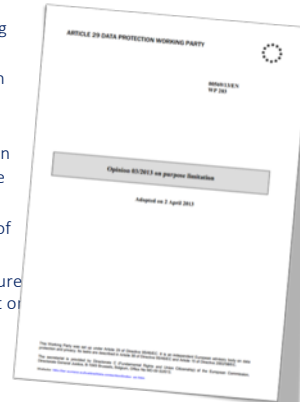
- personal data which airlines gathered about their passengers for flight purposes cannot subsequently be used by immigration services at the destination
- Achmea and Albert Heijn

36

purpose limitation

A substantive compatibility assessment requires an assessment of all relevant circumstances. In particular, account should be taken of the following key factors:

- the relationship between the purposes for which the personal data have been collected and the purposes of further processing;
- the context in which the personal data have been collected and the reasonable expectations of the data subjects as to their further use;
- the nature of the personal data and the impact of the further processing on the data subjects;
- the safeguards adopted by the controller to ensure fair processing and to prevent any undue impact on the data subjects.



37

purpose limitation

A substantive compatibility assessment requires an assessment of all relevant circumstances. In particular, account should be taken of the following key factors:

- the relationship between the purposes for which the personal data have been collected and the purposes of further processing;
- the context in which the personal data have been collected and the reasonable expectations of the data subjects as to their further use;
- the nature of the personal data and the impact of the further processing on the data subjects;
- the safeguards adopted by the controller to ensure fair processing and to prevent any undue impact on the data subjects.

legitimate interest...

factors to consider when carrying out the balancing test:

- nature and source of the legitimate interest and whether the data processing is necessary for the exercise of a fundamental right, is otherwise in the public interest, or benefits from recognition in the community concerned;
- impact on the data subject and their reasonable expectations about what will happen to their data, as well as the nature of the data and how they are processed;
- additional safeguards which could limit undue impact on the data subject, such as data minimisation, privacy-enhancing technologies; increased transparency; general and unconditional right to opt-out, and data portability

38

purpose specification and limitation

collection for specified, explicit and legitimate purposes

not further processed in a manner that is incompatible with those purposes

Art. 5(1)b en 6(4) AVG

- relation between the purposes for which the personal data have been collected and the purposes of the further processing
- context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller (expectations)
- nature of the personal data, in particular whether special categories of personal data are processed,
- consequences of the intended further processing for data subjects;
- appropriate safeguards



39

presumption of compatibility

processing for

- archiving purposes in the public interest
- scientific or historical research purposes
- statistical purposes

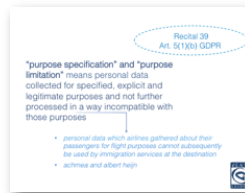
in accordance with art. 89(1) GDPR

40

Art. 5(1)(c) GDPR

“data minimisation” means personal data is adequate, relevant, and limited to the minimum necessary in relation to the purposes for which they are processed;

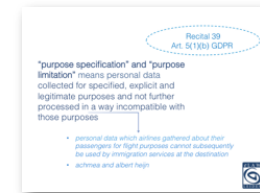
they shall only be processed if, and as long as, the purposes could not be fulfilled by processing information that does not involve personal data



41

Art. 5(1)(e) GDPR

“storage minimisation” means personal data is kept in a form which permits direct or indirect identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed



42

The Problem with Big Data (Or: with Data Protection Law)

transparency (art. 12-14 AVG)

- use of algorithms — profiling (art. 22 AVG)
- opacity of the processing
- tendency to collect 'all data'
- repurposing of data, and — dataminimization (art. 5.1c)
- use of new types of data — purpose limitation (art. 5.1b)

43

Art. 9 GDPR

special (categories) of data

- race or ethnic origin
- political opinions
- religion or philosophical belief
- sexual orientation or gender identity
- trade union membership
- genetic data
- biometric ID-data
- health
- sex life

processing not allowed, unless

- specific exceptions e.g. use of health data by a medical doctor
- general exceptions such as explicit data subject consent, manifestly made public by data subject, legal proceedings, etc.

44

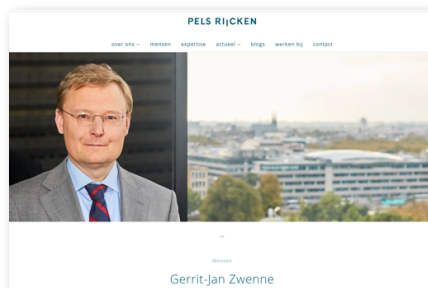
The processing of special categories of personal data is allowed...

- data subject explicit consent
- employment and social security and social protection law
- data subjects' or other individuals' vital interests
- foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aims...
- manifestly made public by data subject
- establishment, exercise or defence of legal claims
- substantial public interest, preventive or occupational medicine, assessment of the working capacity employees, medical diagnosis etc.
- public health or archiving purposes in the public interest, scientific or historical research purposes etc.

45

**date of birth? surname?
photo's? length? IQ?
'three 'vaasjes' Heineken'..?**

46



47

(51) The processing of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person.

Such [special data] personal data should not be processed, unless processing is allowed in specific cases set out in this Regulation, taking into account that Member States law may lay down specific provisions on data protection in order

48

criminal data

Art. 10 GDPR

- data on criminal convictions and offences
- or related security measures

processing only by official authorities, unless

an official public register that shows a medical doctor has been reprimanded (disciplinary measure)...

- specific exceptions e.g. use of criminal data by probation services
- general exceptions such as explicit data subject consent, manifestly made public by data subject, legal proceedings, etc.

49

dentist

- a lot of children do not go to the dentist, because their parents think the dentist is not covered by their health insurance
- but it is!
- can health insurers inform their customers about the dentist coverage?

preferably only customers that did not claim children's dentist cost...

basis for processing?

purpose specification

processing health data?

50

John is a well-paid photo model whose image appears on many websites, online-brochures and the like. One of his friends tells him about his rights as a data-subject. That makes him think. After some additional research he sends one of his clients, a website publisher, a registered letter.

In that letter he states, that

- to the extent the website has his consent to process his personal data (included inter alia in photos of him), he now withdraws such consent, and
- consequently the website is no longer permitted to process his personal data, including the photos of him.

The website asks your advice.

In your advice please take into account the **nature of the data** processed in this context and the requirements for **valid consent**.

Would it make a difference if John is **self-employed** or an **employee** working for an agency?

51

John is a well-paid photo model whose image appears on many websites, online brochures and the like. One of his friends tells him about his rights as a data subject. That makes him think. After some additional research he sends one of his clients, a website publisher, a registered letter.

In that letter he states, that

- to the extent the website has his consent to process his personal data (included inter alia in photos of him), he now withdraws such consent, and
- consequently the website is no longer permitted to process his personal data, including the photos of him.

The website asks your advice.

In your advice please take into account the nature of the data processed in this context and the requirements for valid consent.

Would it make a difference if John is self-employed or an employee working for an agency?

- personal data...?
- **special data...?**
- basis for processing...?
- purpose specification and purpose limitation?

what exceptions to use?

data subject explicit consent?
manifestly made public by the data subject?

What about art. 85 GDPR?

(42) Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.

52

DPA Enforcement

- *in cases of first and non-intentional non-compliance: a warning in writing*
- *regular periodic data protection audits*

a fine up to €10 or 20 mio
or up to 2% or 4% of the
annual worldwide turnover
(whichever is greater)



53

QUIZ

...?

9 The Dutch DPA (DDPA) imposed a fine on tennis association KNLTB for selling the personal data of its members.

In 2018, according to the DDPA, KNLTB unlawfully provided personal data of a few thousand of its members to two sponsors. What was the amount of the fine?

- A. 20 million euro
- B. 10 million euro
- C. 525,000 euro
- D. 52,500 euro



54

questions?

g.j.zwenne@law.leidenuniv.nl

55