

PRIVACY AND EU DATA PROTECTION

*Seminar III. and IV.*

**Main principles. Lawfull processing. Purpose specification and purpose limitation.**

*prof. dr. Gerrit-Jan Zwenne*




September 11<sup>th</sup>, 2019

**But first...**

- Name three examples of national Data Protection Authorities (DPAs) in EU Member States
- Whats is (was) the Article 29 Working Party?
- What is the EDPS (European Data Protection Supervisor)?
- For what reasons was harmonization of national DP-law in the EC/EU necessary?



**Also...**



**personal data**

- is a license plate personal data?
- and: info@companyname.nl?
- and: IPv4: 213.125.106.12?

**processing**

- what is 'processing' ..? what is not?

**data subject, controller and processor**

- you upload photos to a social network: who is/are data subjects? who is/are controller and/or processor?

**And...**

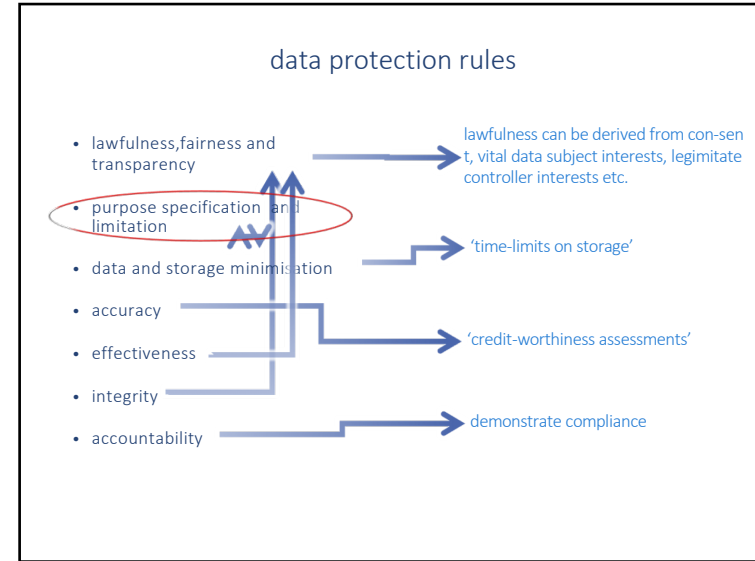
- Koninklijke Philips N.V., a Dutch multinational tech company headquartered in Amsterdam (NL), intends to sell MRI-scanners and LED-lights in China. For that purpose Philips requests the data science department of the University of Mumbay (India) to analyze personal data of board members of Chinese health clinics.
- Cambridge Analytica Ltd based in London (UK) processed personal data of US citizens.
- As of 1st of November 2019, the successor of Cambridge Analytica will process personal data of Dutch citizens in Canada.
- An internet advertising network uses cookies to track from internet-users, inter alia in the Netherlands



Chicago Tribune

Unfortunately, our website is currently unavailable in most European countries. We are engaged on the issue and committed to looking at options that support our full range of digital offerings to the EU market. We continue to identify technical compliance solutions that will provide all readers with our award-winning journalism.

*is this necessary..?*



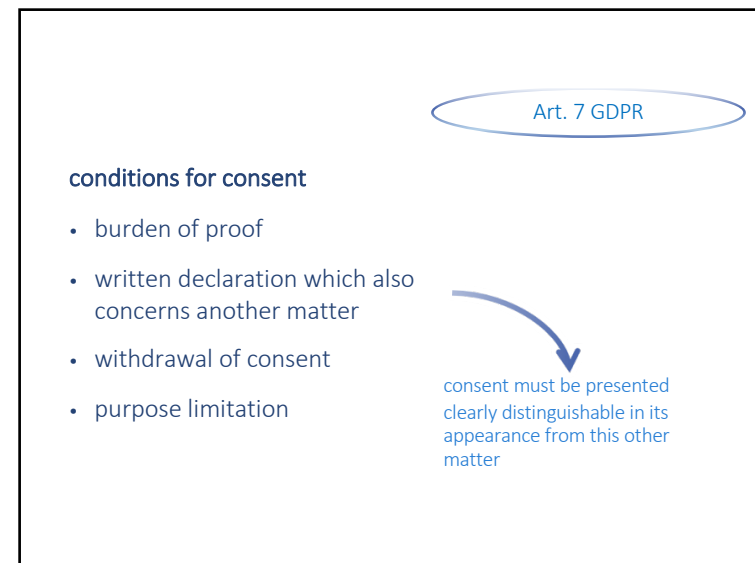
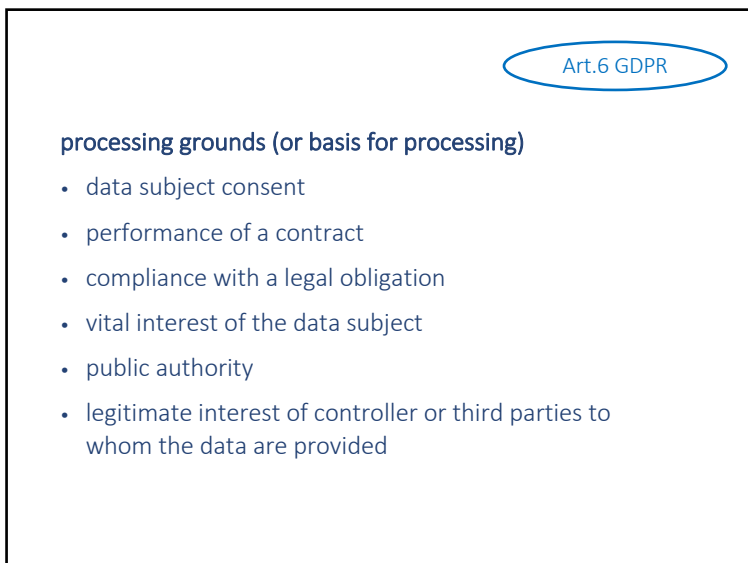
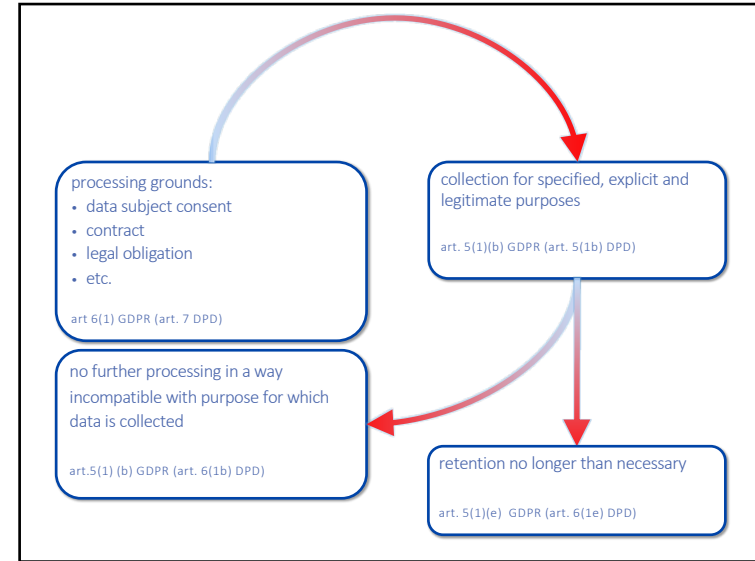
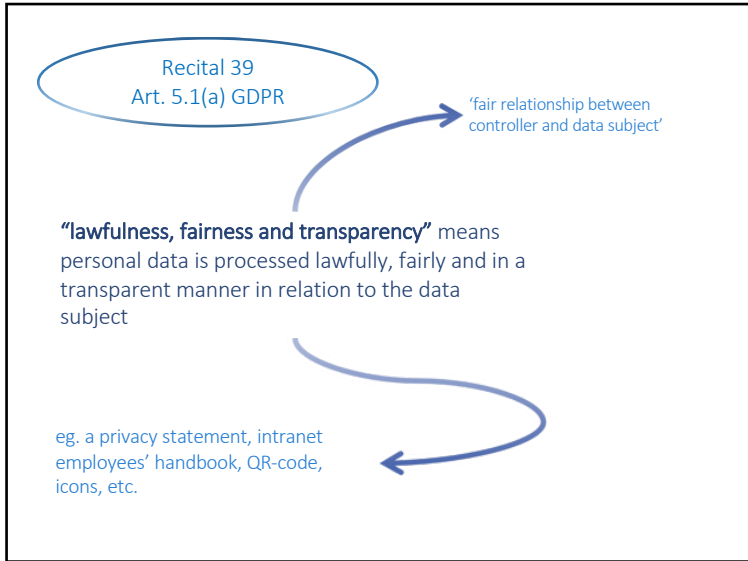
Art. 5(1)(d) GDPR

**“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

**“effectiveness”** means personal data is processed in a way that effectively allows the data subject to exercise his or her rights

Art. 5(1)(f) 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



**definition**

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

Art. 4 (11) GDPR

Conclusie AG in Planet 49

Art. 2(h)  
RI 95/46

• onduidelzinnige wilsuiting van de betrokkene vereist én

Art. 4(11)  
AVG

• onduidelzinnige wilsuiting van de betrokkene vereist én  
• onduidelzinnige actieve handeling

(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..

(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 in plain language  
what constitutes detriment...?

(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

(43) Consent is **presumed not to be** freely given 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.

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.

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.

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

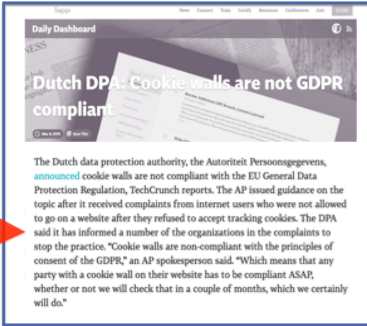
freely given...

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.

without detriment....


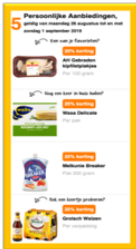
(42) Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent *without detriment*.



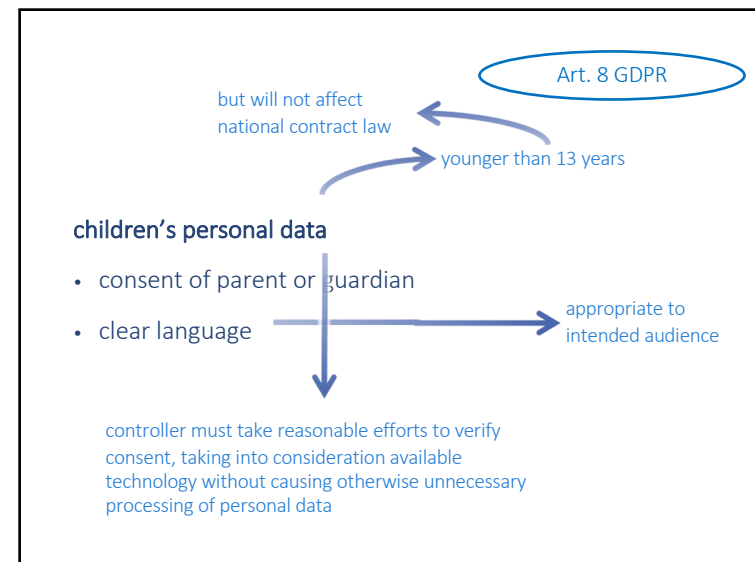
The Dutch data protection authority, the Autoriteit Persoonsgegevens, announced cookie walls are not compliant with the EU General Data Protection Regulation, TechCrunch reports. The AP issued guidance on the topic after it received complaints from internet users who were not allowed to go on a website 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."

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?


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





won't somebody please think of the children!?

vital interests



### 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?

proportionality & subsidiarity

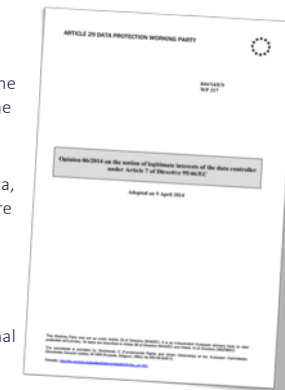
the balance between the processing's effects on the interest of the controller on the one hand and the impact on the data subjects' interests

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

### 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



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

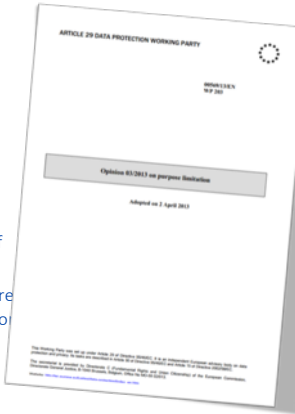
**“purpose specification” and “purpose limitation”** means personal data collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes

- 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

### 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 of the data subjects.



### purpose limitation

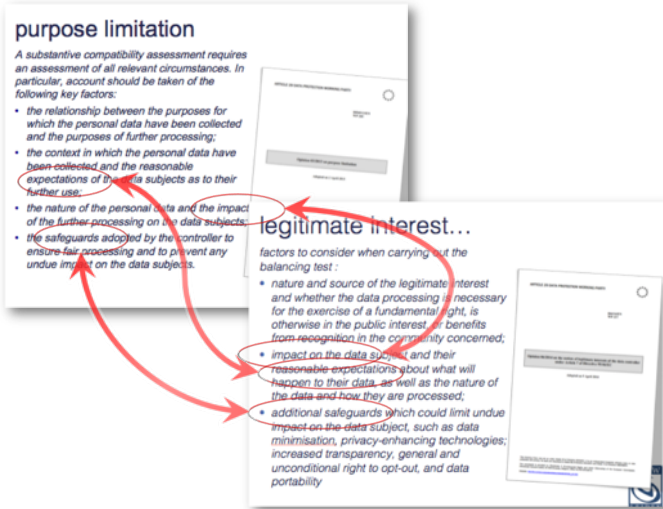
A substantive compatibility assessment requires an assessment of all relevant circumstances. In particular, account should be taken of the following key factors:

- 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




### 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





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

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

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

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)

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.

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.

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

PELS RIJCKEN

Teng Hoer Sla

PELS RIJCKEN

Gerrit-Jan Zwenne

(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

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.

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?*

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?

?

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 in the photo 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 about art. 85 GDPR?

what exceptions to use?


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

(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.

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)



questions?

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