

LAW AND DIGITAL TECHNOLOGIES
INTERNET PRIVACY AND EU DATA
PROTECTION

Principles and Rules for
Processing Personal Data

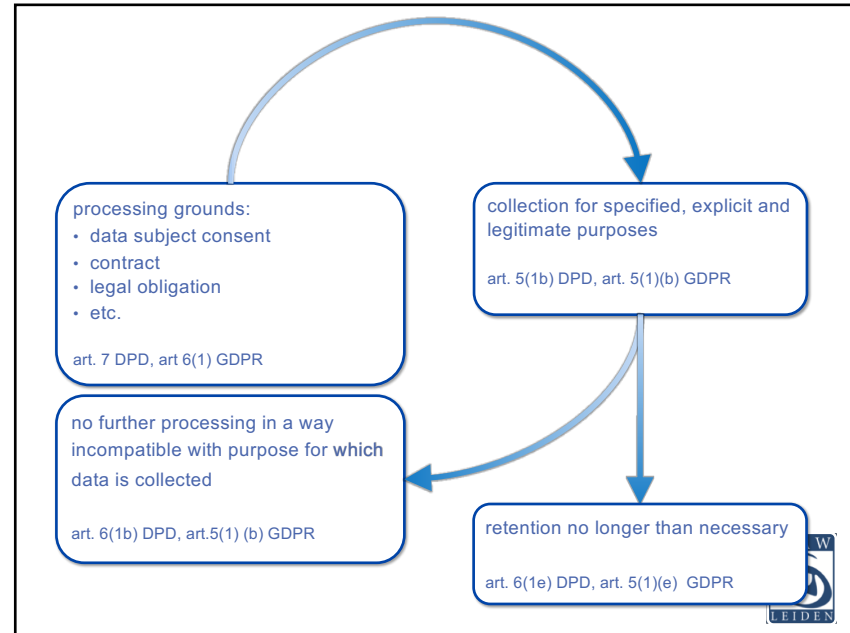
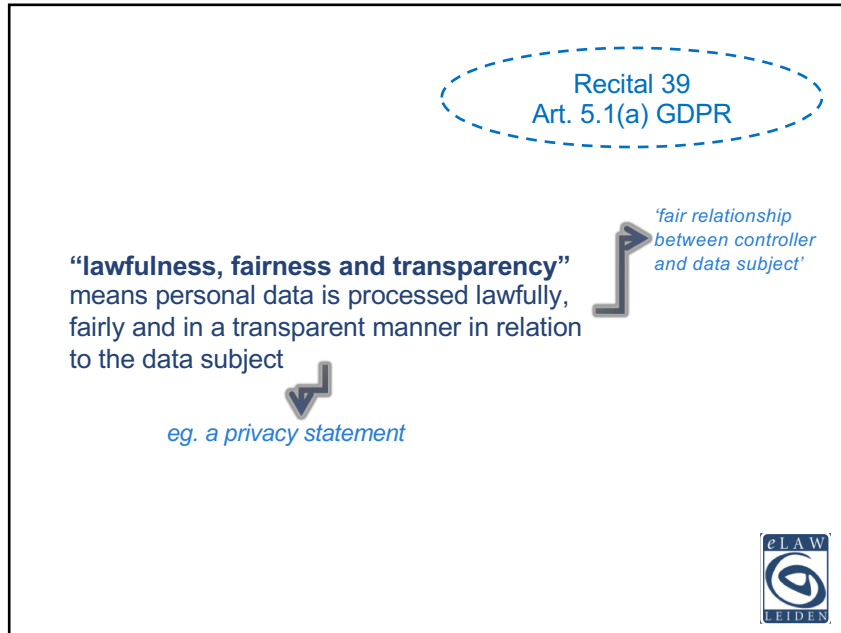
Gerrit-Jan Zwenne
Seminar III
October 31th, 2018



data protection rules

- lawfulness, fairness and transparency → *lawfulness can be derived from consent, vital data subject interests, legitimate controller interests etc.*
- purpose specification and limitation → *'time-limits on storage'*
- data and storage minimisation → *'credit-worthiness assessments'*
- accuracy → *'demonstrate compliance'*
- effectiveness → *'demonstrate compliance'*
- integrity → *'demonstrate compliance'*
- **accountability** → *'demonstrate compliance'*






Art.6 GDPR

lawfulness of 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




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




(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 an 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

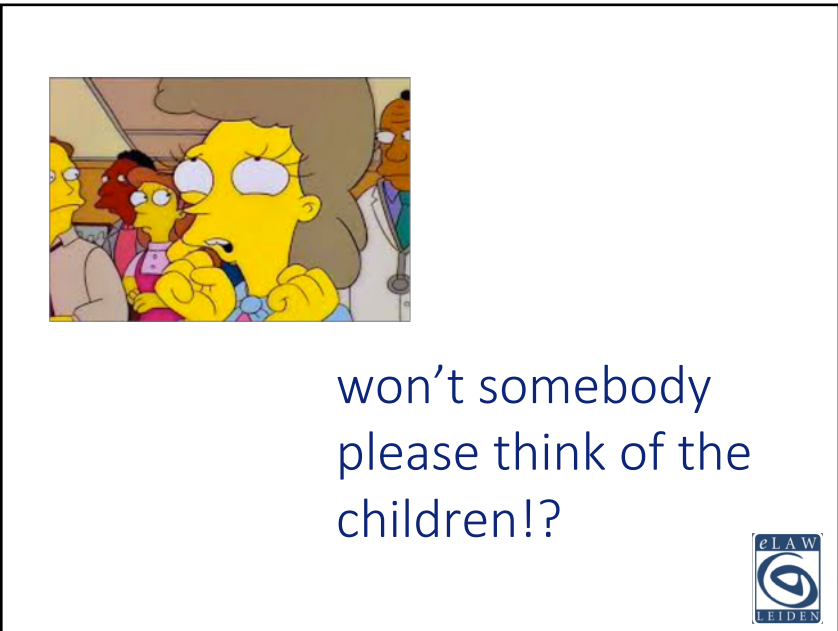
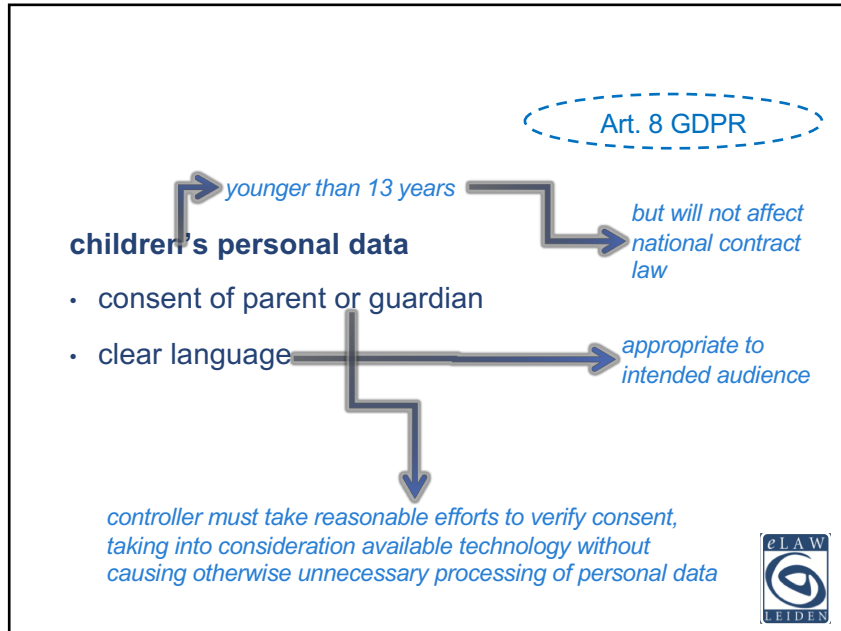
seems much stricter than art. 7.4 GDPR

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.



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





vital 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

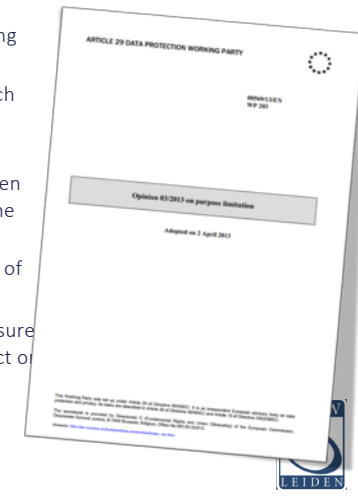
- *personal data which airlines gathered about their passengers for flight purposes cannot subsequently be used by immigration services at the destination*
- *achmea and albert heijn*



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 on 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



Art. 5(1)(c) G
DPR

“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

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

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

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

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




Art. 5(ea) GDPR

“**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



Art. 9 GDPR


special (categories) of data

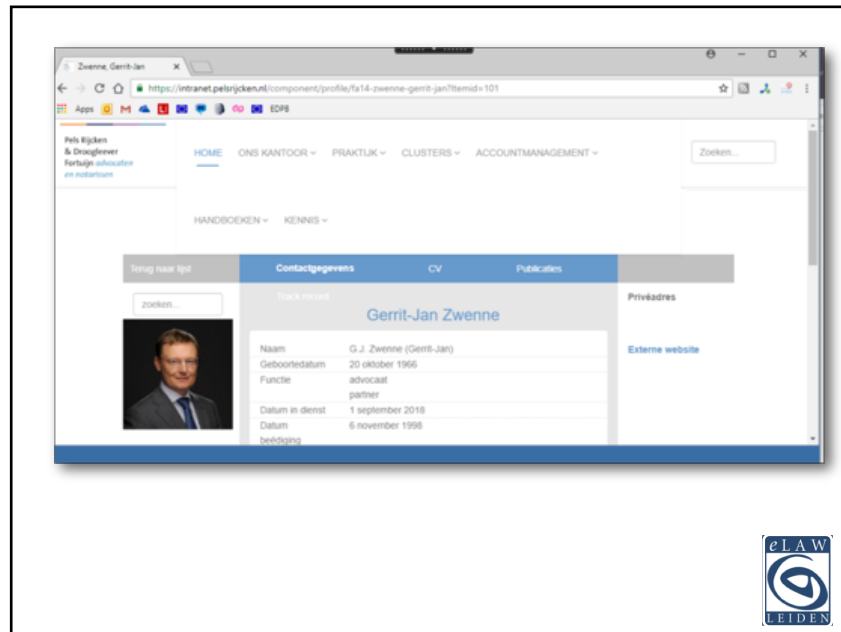
- race or ethnic origin
- political opinions
- religion or philosophical belief
- sexual orientation or gender identity
- trade union membership
- genetic data
- biometric ID-data
- health
- sex life

date of birth
length, weight
passport photo ?

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.



(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



- 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)*



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?



questions?

g.j.zwenne@law.leidenuniv.nl

