universität wien

From the GDPR to the AIA – problems solved?

Christiane Wendehorst

PANELFIT Conference, Vienna, 28 March 2022

universität wien

1 The GDPR – a ‘gold standard’ and its problems

2 ‘Data sharing legislation’: trying to turn the tide

3 Completing the picture? Towards the AI Act

GDPR – the gold standard of data protection?

- Arguably the most influential piece of EU legislation
- Inspired lawmaking worldwide
- Stands for the ‘gold standard’ in data protection
- Perceived as offering the highest level of protection possible

Problems with the GDPR I: consent

Problem no. 1: consent

I have read the privacy policy and agree with all its terms.

Problem no. 1: consent

Article 4

Definitions

For the purposes of this Regulation: …

(11) 'consent' of the data subject means 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 dat relating to him or her;

No mentioning of substantive limits (unacceptable risks for data subject and others, including society at large)

Problem no. 1: consent

Article 5

Principles relating to processing of personal data

1. Personal data shall be:
   a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

… just some vague reference to fairness, but only as a general principle …

Recitals:

(42) Where processing is based on the data subject's consent, ... In accordance with Council Directive 93/13/EEC a declaration of consent pre- formulated by the controller should … not contain unfair terms.

…

… or is it all left to the Unfair Contract Terms Directive?

Problem no. 1: consent

Article 13

Information to be provided where personal data are collected from the data subject

1. Where personal data … are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information: …
   (a) the identity and the contact details of the controller and, where applicable, of the controller's representative;
   (b) the contact details of the data protection officer, where applicable;
   (c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
   (d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;
   (e) the recipients or categories of recipients of the personal data, if any;
   (f) where applicable, the fact that the controller intends to transfer personal data to a third country ….

The most important information for the data subject is missing: what is the inherent risk?
(E.g. does the purpose of 'personalisation of content and offers' mean I will waste less time searching in the WWW, or does it mean I will always pay the maximum price I can still afford)

Problem no. 1: consent

Recitals:
(32) Consent should be given … , 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, ….

No information or confirmation on a durable medium – one click, and it's over and can no longer be traced by the data subject …

… and there is no time limit, i.e. the one click takes effect for ever and ever …

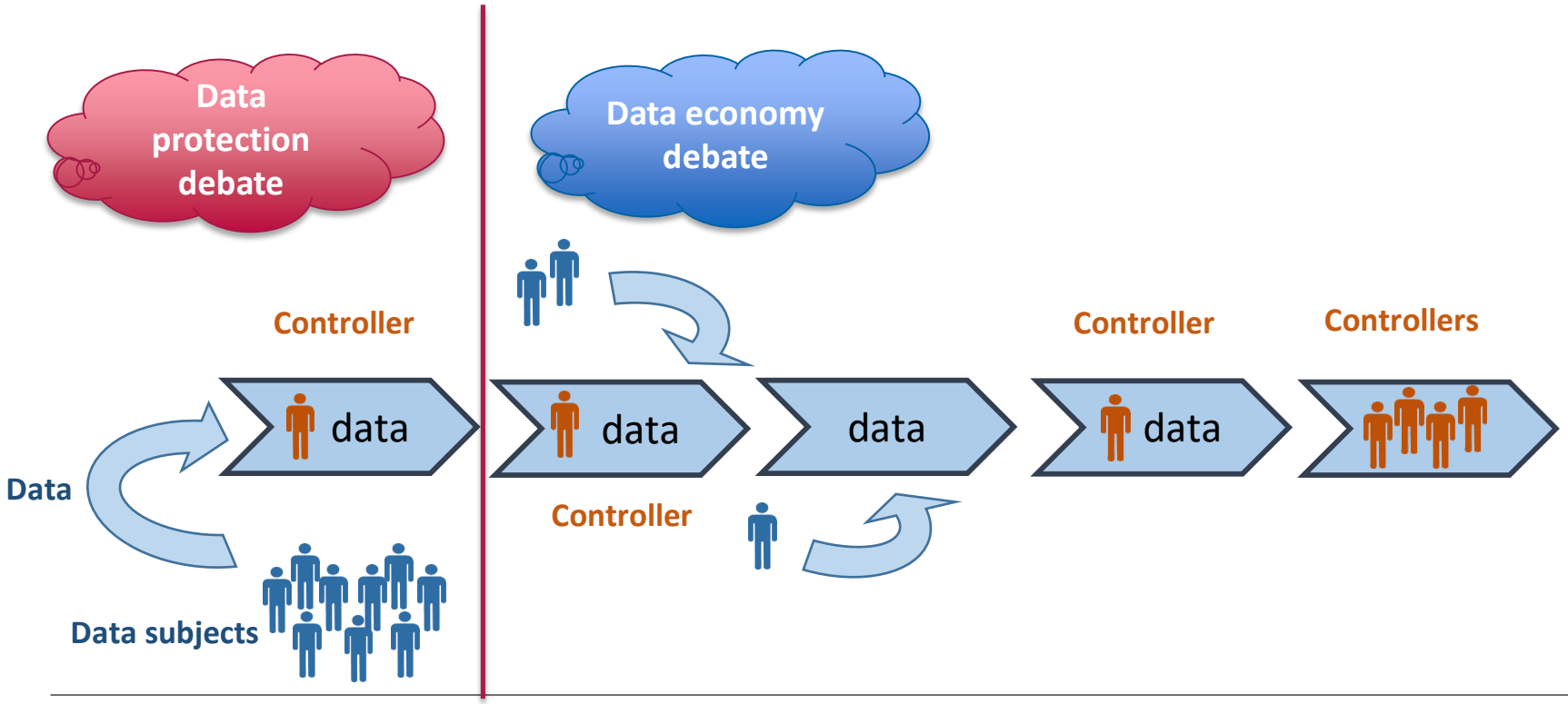
Article 13

Information to be provided where personal data are collected from the data subject

1. Where personal data … are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information: …

Problems with the GDPR II: even less protection where data is passed on

Problem no.2: onward transfer



Problem no.2: onward transfer

Article 30

Records of processing activities

1. Each controller… shall maintain a record of processing activities under its responsibility. That record shall contain …:

   (d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations; …

Only 'categories ' mentioned
(same for information duties)

What if the records only show the 'categories', and what is 'disproportionate effort'?

Article 19

Notification obligation regarding rectification or erasure of personal data or restriction of processing

The controller shall communicate any rectification or erasure of personal data or restriction of processing …to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. ….

Problem no.2: onward transfer

Secondary use, including by onward transfer, only subject to compatibility test *(where not already included in consent)*

Recitals GDPR:

(50) The processing of personal data for purposes other than those for which the personal data were initially collected should be allowed only where the processing is compatible with the purposes for which the personal data were initially collected. **In such a case, no legal basis separate from that which allowed the collection of the personal data is required.** ….

Can we achieve the desired protection by way of reference to general principles?

Article 6

…ess of processing

…

4. … the controller shall, in order to ascertain whether processing for another purpose is compatible … take into account, inter alia: ….
   e) the **existence of appropriate safeguards**, which may include encryption or pseudonymisation.

Problem no.2: onward transfer

Processor

1. Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.

2. The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.

3. Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects obligations and rights of the controller. That contract or other legal act shall stipulate, in particular,

(a) processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;

(b) ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

(c) takes all measures required pursuant to Article 32;

(d) respects the conditions referred to in paragraphs 2 and 4 for engaging another processor;

(e) taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;

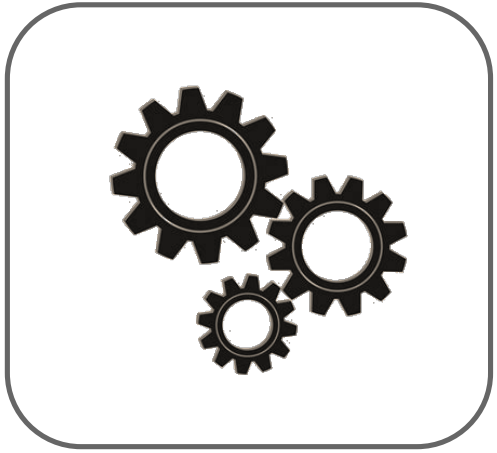
(f) assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account

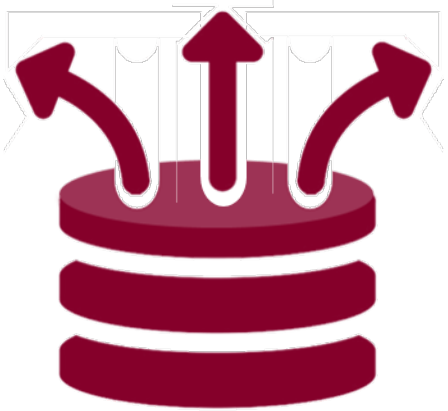
Articles 28 et seq include very detailed rules on the controller's duties with regard to onward transfer to processors

A counterpart for controller-to-controller transfers is missing.

Problems with the GDPR III:
a blind eye on the algorithm perspective

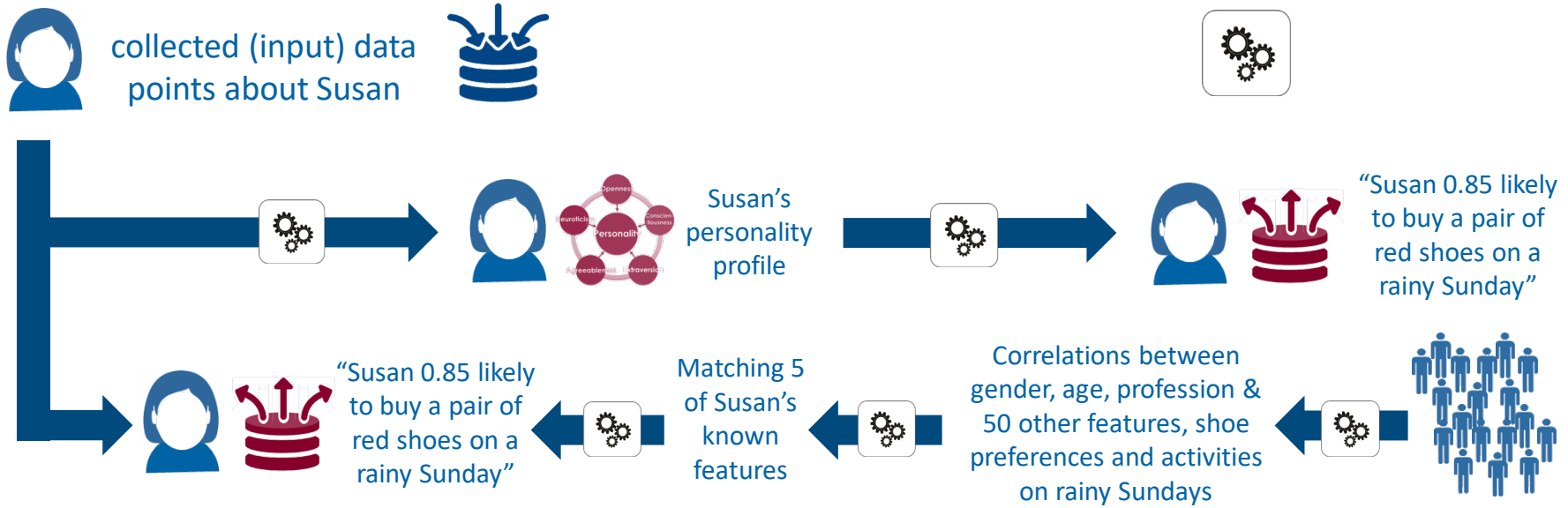
Problem no. 3: algorithm perspective





(Input) data **+** **Algorithm** **=** **(Output) data**

Problem no. 3: algorithm perspective



The GDPR's focus on the bilateral relationship between a data subject and the controller fails to reflect the multi-relational nature of data and data use, i.e. any provision of data by one person (and many others) affects also individuals who have provided hardly any data about themselves.

Problem no. 3: algorithm perspective

collected (input) data points about Susan

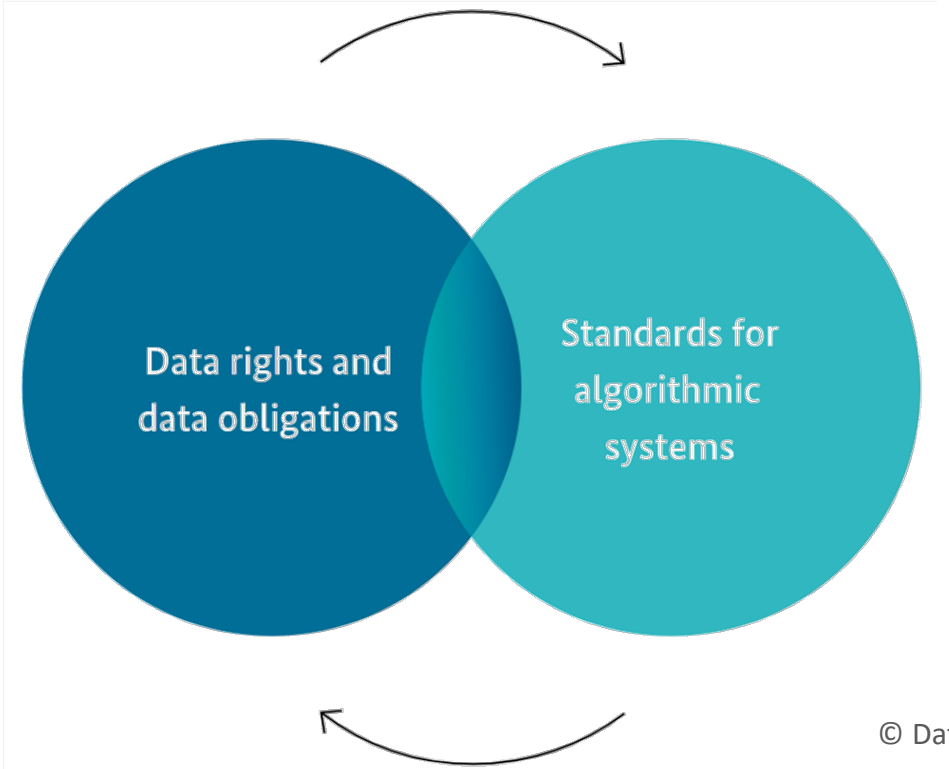
Susan's personality profile

"Susan 0.85 likely to buy a pair of red shoes on a rainy Sunday"

The GDPR's focus on existing data, i.e. on data that persist on a medium or are in a state of transmission, fails to reflect the fact that data and algorithms are, to a certain extent, interchangeable and that extremely few input data points may, depending on the algorithm used, lead to highly problematic outcomes.

"Display pair of red shoes now!"

Data perspective & algorithm perspective



Problem no. 3: algorithm persp

Article 22 (with corresponding information duties in Articles 13 to 15) as the only provision on algorithm perspective

Article 22

Automated individual decision-making, including profiling

1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.
2. Paragraph 1 shall not apply if the decision:
   (a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;
   (b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or
   (c) is based on the data subject's explicit consent.

....

Rather narrow in scope

Why we need a paradigm shift

Why we need a paradigm shift

- Protection through the GDPR has **serious gaps**, in particular where data is **passed on** by the initial controller, and where **algorithms** replace data.
- The **paradigm of informed consent has largely failed** – because of information overload, absence of information as to the risks involved, absence of realistic alternatives, lack of documentation, potentially 'eternal' duration, …
- One important step is to **improve the rules on consent**, in particular to ensure machine-readable documentation, automatized traceability along the chain, validity only for a limited duration, and administration according to the data subject's consent with the help of PIMS and PMT, …

Why we need a paradigm shift

- … however, it may be the focus on consent, agency etc itself that is moving in the wrong direction – maybe what we need to achieve instead is **rational indifference** (as we did in contract law thanks to the Unfair Contract Terms Directive, UCTD), i.e. individuals can click as many buttons as they like without reading too much of privacy policies and still trust that nothing really harmful will happen.
- This can be achieved by a blacklist of **unfair data practices/unfair algorithmic practices**, combined with general clauses, which are prohibited per se and cannot be overcome by consent (or only by consent that is highly individualised and formalised).

Why we need a paradigm shift

- Also from the perspective of businesses and organisations that want to use data consent is problematic as there is always the danger consent will be found ineffective by a court later.
- Immense legal uncertainty and compliance costs even for data activities with no or minimal risk for data subjects has a chilling effect and is likely to push SMEs out of the market.
- Safe harbours for businesses and organisations that engage in data use with no relevant risk for the data subject (e.g. small-scale processing, many forms of use in the context of training AI) could be created by way of a **whitelist of selected fair data practices/algorithmic practices**.

Why we need a paradigm shift

universität wien

Legitimate data use
statutory legal basis

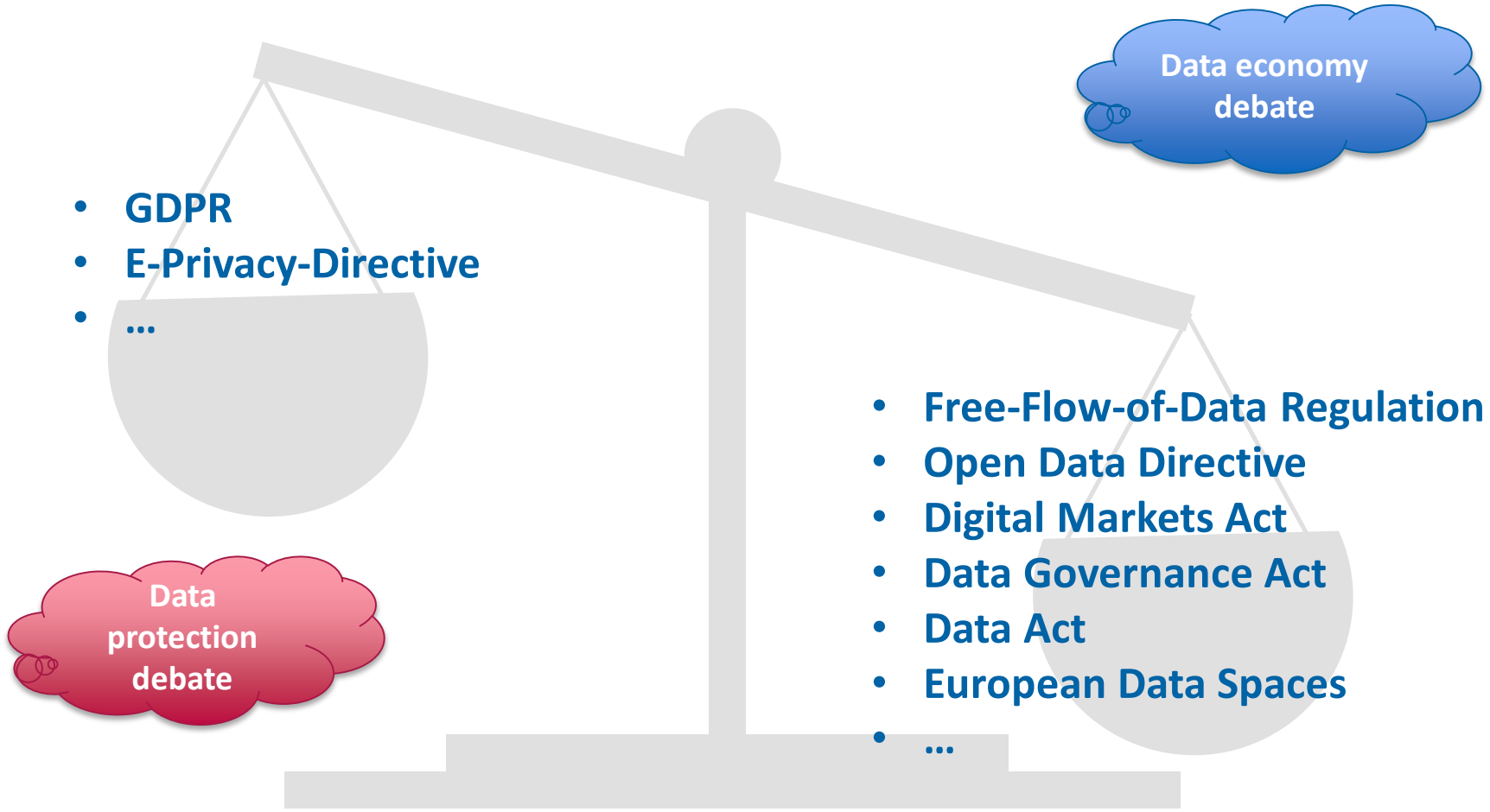
Fair data practices
Fair algorithmic practices

Data use which can get a legal basis by way of consent

Prohibited data use
no consent possible

Unfair data practices
Unfair algorithmic practices

Data sharing legislation: trying to turn the tide


Data economy debate
GDPR
E-Privacy-Directive
…
Free-Flow-of-Data Regulation
Open Data Directive
Digital Markets Act
Data Governance Act
Data Act
European Data Spaces
…
Data protection debate

A competing gold standard

Completing the picture?
Towards the AI Act

EUROPEAN
COMMISSION

universität
wien

Brussels, 21.4.2021
COM(2021) 206 final

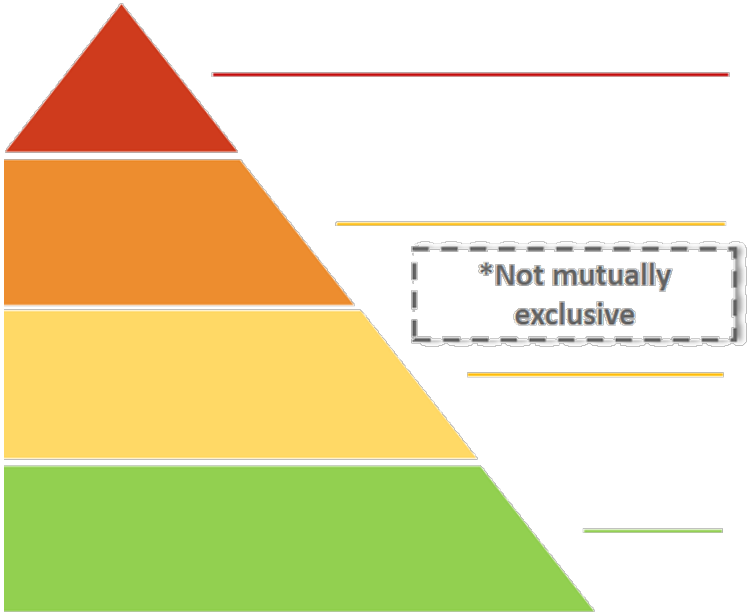
2021/0106 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS

The risk-based approach



*Not mutually exclusive

Unacceptable risk
e.g. social scoring

Prohibited

High risk
e.g. recruitment, medical devices

Permitted subject to compliance with AI requirements and ex-ante conformity assessment

'Transparency' risk
'Impersonation' (bots)

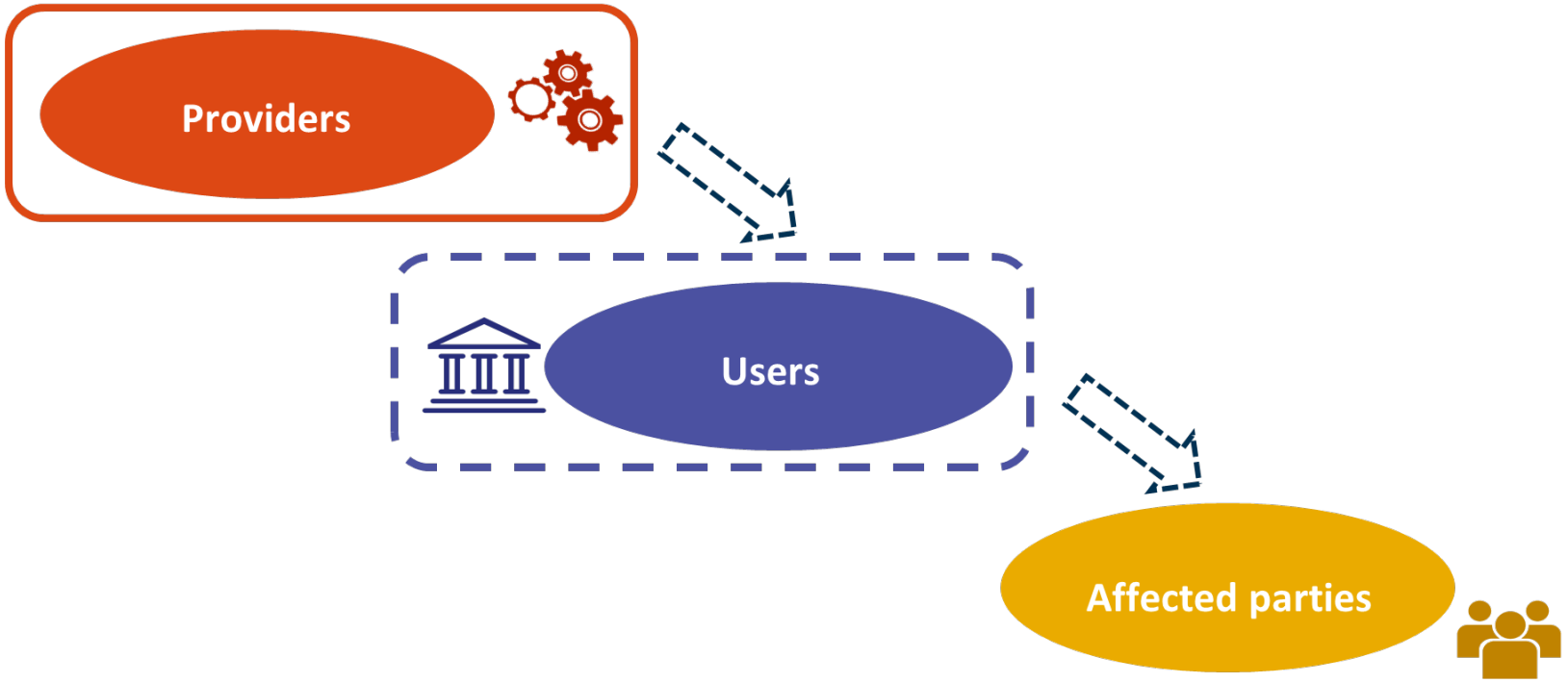
Permitted but subject to information/transparency obligations

Minimal or no risk

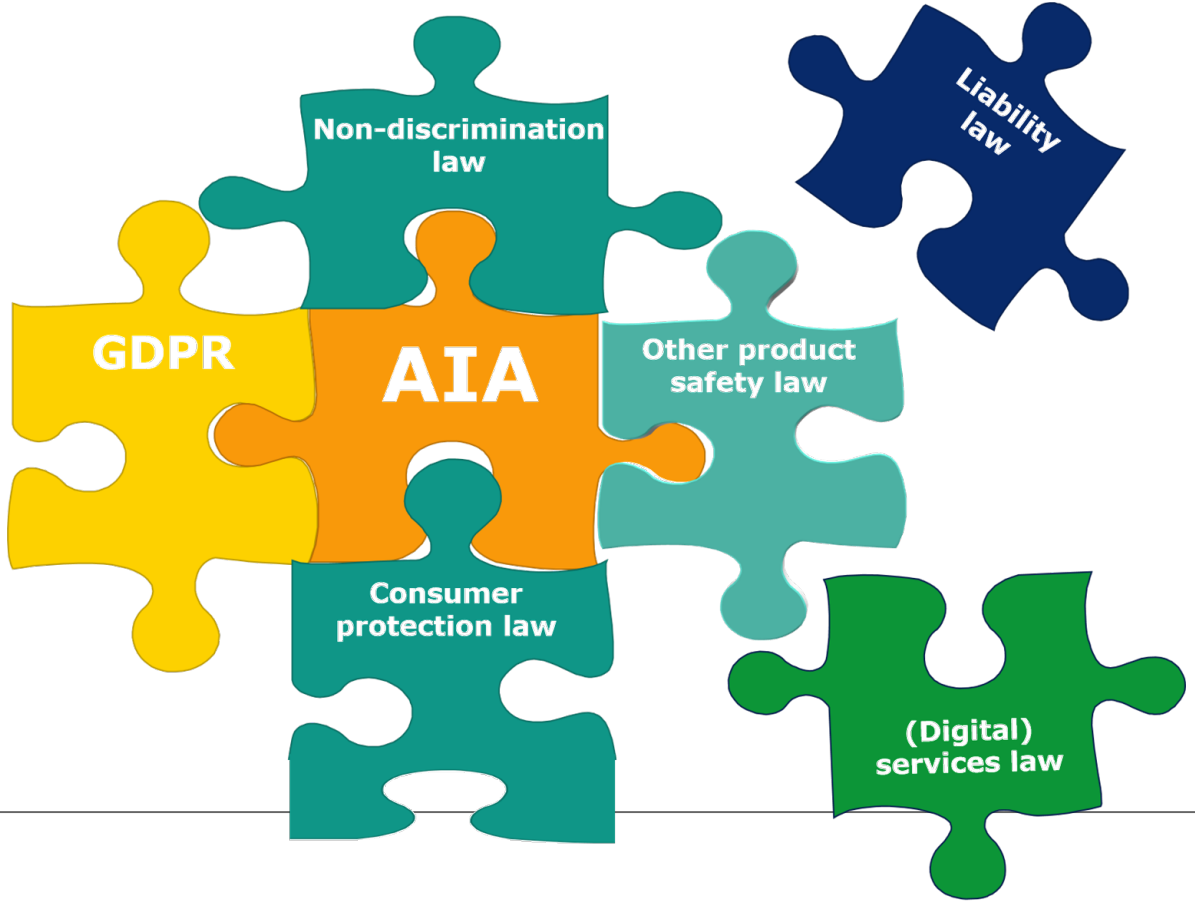
Permitted with no restrictions

European Commission

The product safety law approach



Interplay with GDPR and other laws



Problems solved?

universität wien

Consent ☐

AI Act lists some prohibited AI practices, which is good, but the list is very narrow. Significance of the law on unfair contract terms and unfair commercial practices still largely unclear.

Onward transfer ☐

Made rather worse by data sharing legislation. Data Governance Act stresses role of intermediaries, but level of protection not very high. Data Act contains some additional protection, but mainly for non-personal data.

Algorithms ☐

AI Act establishes product safety regime for high-risk AI, which is good, but scope is rather narrow. Fails to include individual rights and largely relies on GDPR.

Uncertainty ☐

Only very punctual improvements, e.g. on use of sensitive data categories for running bias checks, and possibly by encouraging use of data intermediaries

Conclusions

- The GDPR is a beautiful masterpiece of legislative craftsmanship, which has served to raise awareness with regard to data protection and influence law-making worldwide as a ‘gold standard of protection’, but it comes at a high price.
- At a closer look, the level of protection afforded by the GDPR turns out not to be very high after all. While its provisions might be applied by courts in a way that really makes a difference, such application is difficult to predict, most likely not very targeted and might have unintended effects on the European digital economy.
- Conversely, the GDPR has caused unprecedented administrative burden and legal uncertainty for more or less any kind of activity, without regard to the risk actually created.

Conclusions

- The European legislator has reacted by enacting or proposing a patchwork of ‘data sharing legislation’, striving towards the new gold standard of ‘open by default’. It seeks to enhance data portability and other forms of data sharing. The relationship with the GDPR is largely unclear (‘without-prejudice-to’ formula)
- With the proposed AI Act, the European Commission is trying not to repeat the mistakes made earlier and to take a strictly risk-based approach.
- There are many positive aspects of the AI Act, but it fails to solve most of the problems created by the GDPR. There may thus, in the long run, be no alternative to re-opening the GDPR debate and to revising the ‘gold standard’.