

EDM and GDPR

FACT about General Data Protection Regulation

prof. dr. Mykola Pechenizkiy

<http://www.win.tue.nl/~mpechen/>

EDM2018 Workshop: Policy & EDM: Norms, Risks, and Safeguards

15 July 2018

The EU General Data Protection Regulation (GDPR) is the most important change in data privacy regulation in 20 years - we're here to make sure you're prepared.

Penalties

Under GDPR organizations in breach of GDPR can be fined up to 4% of annual global turnover or €20 Million (whichever is greater). This is the maximum fine that can be imposed for the most serious infringements e.g. not having sufficient customer consent to process data or violating the core of Privacy by Design concepts. There is a tiered approach to fines e.g. a company can be fined 2% for not having their records in order (article 28), not notifying the supervising authority and data subject about a breach or not conducting impact assessment. It is important to note that these rules apply to both controllers and processors -- meaning 'clouds' will not be exempt from GDPR enforcement.

GDPR Portal: Site Overview

This website is a resource to educate the public about the main elements of the General Data Protection Regulation (GDPR)

Quick Links

[GDPR Key Changes](#)
Summary of key changes



Privacy and Misuse in Automated/ADM

Lawful basis for processing

- an explicit consent (can be withdrawn any time) of the subject for data collected and each purpose data is used for or
- at least one legal basis to do so

Responsibility and accountability

- disclosure of any (solely algorithmic) ADM
- right to view their personal data and how it is being processed

Data protection by design and by default

- privacy settings, encryption
- report any data breaches within 72 hours

EU-level recommendations

- **Tech:** Establish means, measures and standards to assure that ADM systems are fair
- **Ethics:** Ensure that Ethics remain at the forefront of, and integral to, ADM development and deployment.
- **Edu:** Promote value-sensitive ADM design: social values and the ethical priorities of technology users must be designed into all aspects and elements of ADM. Expand the public's awareness and understanding of ADM and its impacts.
- **Legal:** Define clear legal responsibilities for ADM's use and impacts
- **Economic:** Ensure that the economic consequences of ADM adoption are fully considered
- **Societal:** Mandate that all privacy and data acquisition practices of ADM deployers be clearly disclosed to all users of such systems.

Relevant (inter)national research

RESPONSIBLE DATA SCIENCE



<http://www.responsibledatascience.org/>
<https://fatconference.org/>

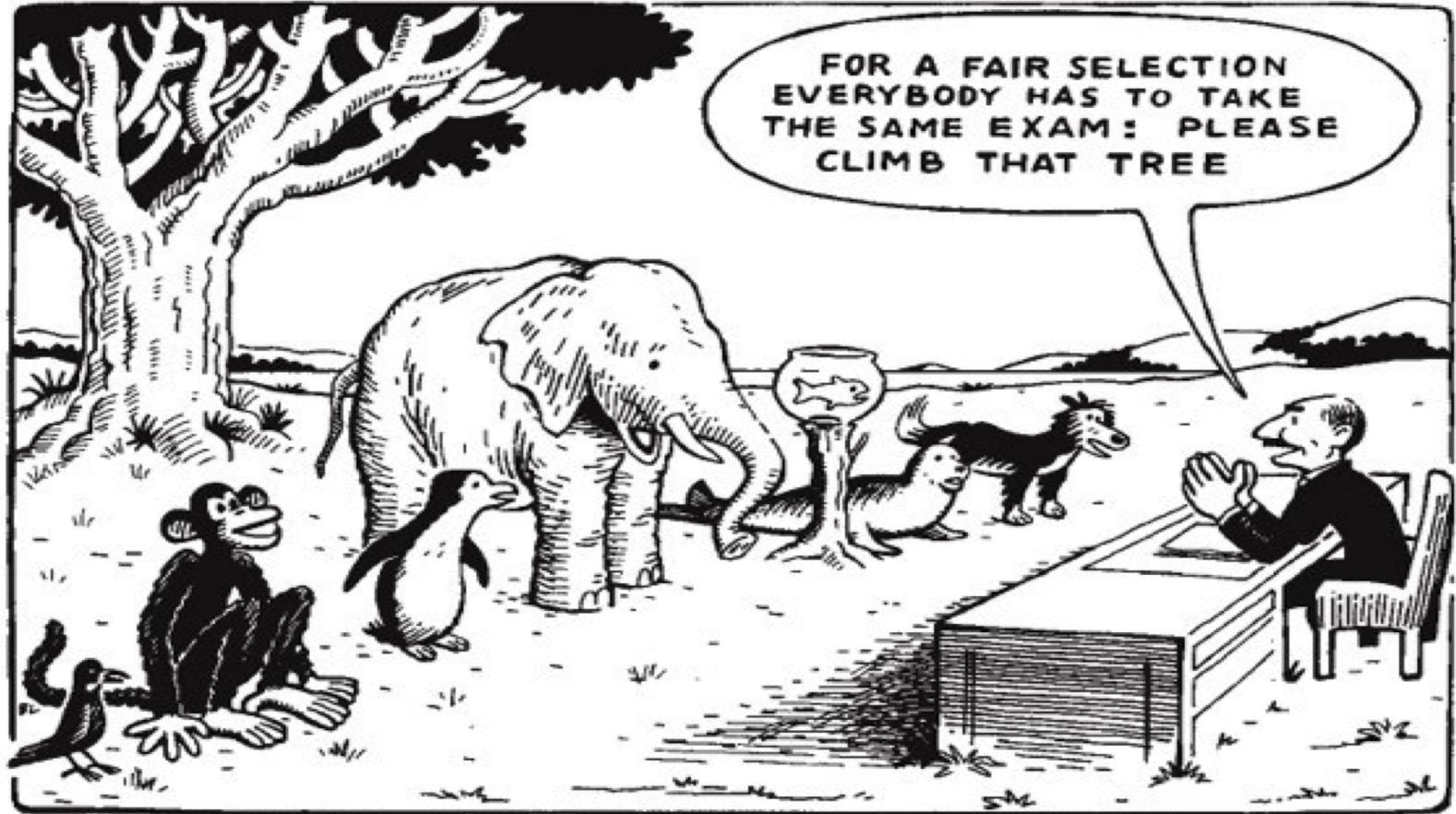
GDPR is already in effect as of May 25

But it is not-trivial to operationalize

- Technically
- Legally

and to bridge the gap between tech and legal perspectives

Different notions of fairness



Auditing model performance for biases in prediction-based decisions

Detecting, measuring and preventing unfair / discriminating decision making or profiling



















Non-uniform accuracy

$$\text{Error}_{\text{males}} \ll \text{Error}_{\text{females}}$$

Favoritism in making decisions:

$$P(+ | \text{male}) - P(+ | \text{female})$$

#GenderShades

Gender Classifier	Darker Male	Darker Female	Lighter Male	Lighter Female	Largest Gap
 Microsoft	94.0% 	79.2% 	100% 	98.3% 	20.8% 
 FACE++	99.3% 	65.5% 	99.2% 	94.0% 	33.8% 
 IBM	88.0% 	65.3% 	99.7% 	92.9% 	34.4% 

- companies did not report how well their products perform across gender, skin type, ethnicity, age or any other attributes
- IBM and Microsoft responded within a day after being informed
- By the time the paper was presented at FAT'18 the companies reported on the internal investigation and **improved performance** of their models

Are men better drivers than women?



- Actual driving behavior data is not available
- Strong patterns can be found from claims
- It is economically rational to use gender to assess risks
- But, there is legislation ...

Why explainable? GDPR

GDPR 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.
3. In the cases referred to in points (a) and (c) of paragraph 2, the data controller **shall implement suitable measures** to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.
4. Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in [Article 9\(1\)](#), unless point (a) or (g) of [Article 9\(2\)](#) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

Interpreting models / outputs

Feature impact on decisions, looking inside the models, “right for a meaningful explanation”, linking to evidence that may explain a decision