

Data protection in the era of AI – the quest for algorithmic accountability

Tuesday 07.12.2021

Webinar JM CoE – Digi-ConSME

Prof. Eleni Kosta
Professor of Technology Law and Human Rights



1

Overview

2

- 1 Key definitions
- 2 Data protection principles
- 3 Grounds for data processing
- 4 Information rights and automated decision making
- 5 Draft AI Regulation



2

3

Personal data

- ✓ **Personal data** means any information relating to an **identified** or **identifiable natural** person: name, email address, shipping address, credit card number, individual purchase history, customization, attendance to events, etc
- ✓ Including by reference to an identifier (introducing a criterion of “singling out”): cookies, IP-addresses, keycoded/pseudonymized data such as lists of consumers whose name is replaced by a serial number or hash
- ✓ **Sensitive data**: medical and health-related, racial or ethnic origin, political opinion, religious or philosophical beliefs, trade union membership, genetic and biometric data, criminal convictions and offenses

3

4

- Truly **anonymous** data are not personal data (0% chance of re-identification)
 - In most cases: still some % chance of re-identification
 - Therefore: supervisory authorities generally consider anonymization a security measure, rather than a measure to render personal data no longer subject to GDPR
- **Public** information remains personal data (i.e. the GDPR still applies to data you pull off public sources, e.g., social media)
- **Pseudonymous** data remain personal data
- **Aggregation** (e.g. 80% of people prefer XYZ) can be a means to take personal data out of realm of GDPR

4

5

Processing

- ✓ **any operation/activity performed on personal data**
- ✓ collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of personal data

Remember, processing thus includes:

- Transfers - including remote access!
- Mere access
- Mere storage
- The process of deletion or anonymization

5

6

Controllers & processors

Controller

- “**determines** the **purposes** and **means** of the processing of personal data”
- i.e. the company processes personal data on its own behalf, for its own business purposes, and therefore ‘controls’ the data, e.g.
 - Collects profile information about consumers
 - Sends targeted emails to those consumers to market company products
 - Performs data analytics to single out key influencers for company promotion
 - Tracks how visitors interact with company website and mobile apps

Processor

- “**processes** personal data **on behalf of the controller**”
- i.e. the controller’s service provider that processes personal data on the instruction and on behalf of the controller, e.g.
 - hosts mobile app data of consumers on behalf of the company (controller)
 - sends marketing emails to consumers on behalf of company (controller)
 - performs website analytics and provide the results to company (controller) for its sole use
 - provides call center support for consumers of the company (controller)

6

7

Lessons to take home

Remember these key definitions

- Remember that nearly all marketing activities involve personal data
- For which the controller is responsible
- That includes information that is from public sources
- And information that does not directly reveal the individual's identity
- True anonymization is very hard to achieve, so if someone claims data are anonymized, contact your DPO for verification

7

8

Categories of big data/ analytics/ profiling

❖ Business Intelligence

- Creation of aggregated trend reports **on how products or services are generally used** (not related to identified or identifiable individuals)

❖ Targeted Marketing

- Use of profiling for personalised direct marketing based **on preferences**, such as personalised offers via direct email or in-site targeted advertisement;

❖ Targeted Decision Making


- use of profiling **for purposes of taking decision about individuals**, e.g. decide on the granting of a loan. This category may also apply if e.g. results of Business Intelligence are applied to differentiate between individuals or segments of individuals (e.g. applying differentiated pricing).

8

9

Overview

- 1 Key definitions
- 2 Data protection principles
- 3 Grounds for data processing
- 4 Information rights and automated decision making
- 5 Draft AI Regulation




TILBURG UNIVERSITY

9

10

Principles

- Fairness, lawfulness and Transparency
- Purpose limitation
- Storage limitation
- Accuracy
- Data minimisation
- Security, integrity and confidentiality



TILBURG UNIVERSITY

10

11

Lawfulness and fairness

The algorithm and its use shall be lawful and fair, including not unlawfully **discriminatory** and is not unlawfully **biased**:

- ✓ Initial and repeated assessment of the used data sets to check for **unlawful bias**;
- ✓ Addressing **prejudicial elements**, such as over-reliance on correlations without proven causality;
- ✓ Procedures to **prevent** errors, inaccuracies and unlawful discrimination; and
- ✓ Regular **audits** of the algorithm

11

12

Transparency

The data controller must **explain** clearly and simply to individuals **how profiling works** and provide “meaningful information” on the **logic** behind it in its privacy notices.

(S)he should inform the individuals about the **rationale** behind, or the **criteria** relied on when, creating the profile.

* This does not necessarily require a complex explanation of the algorithm used or disclosure of the full algorithm

12

13

Transparency

Ensuring transparency requires:

- ✓ Development of the algorithm in a **predictable and verifiable manner**, so that the data controller can **explain the coding rules** on which the profile is based and is able to justify the relevant decision; and
- ✓ Having a clear understanding of the **information used** in the process, such as the categories of data used for the compilation of the profile and the original source of that information



13

14

Transparency

Challenges raised by ML algorithms:

- ❖ Constantly changing
- ❖ Correlations, no proven causality
- ❖ Cannot be reviewed without training data
- ❖ Sequence of algorithms



14

15

Purpose limitation

Information that was originally collected for a different purpose may not always be used. This requires:

- ✓ a clear **understanding of the information** used in the process and the source of that information;
- ✓ an **assessment of the (types) of available data** that the data controller may use for profiling purposes

15

16

Further processing

Criteria to specify compatible purpose for **further processing**:

- (a) **any link between the purposes** ...;
- (b) the **context** in which the personal data have been collected...;
- (c) the **nature** of the personal data...;
- (d) the possible **consequences** of the intended further processing for data subjects;
- (e) the existence of **appropriate safeguards**, which may include encryption or **pseudonymisation**.

16

17

“Big data analytics” or big data applications for market research seen as ‘statistical purposes’

“The WP29 [...] calls attention to some of the challenges in applying the compatibility test to big data”

- [when organisations processing the data want to detect trends and correlations in the information] notion of **functional separation** (data used for statistical purposes or other research purposes should not be available to ‘support measures or decisions’ that are taken with regard to the individual data subjects concerned)

Art. 29 WP - Opinion 03/2013 on purpose limitation (WP203)

17

18

“[In cases where an organisation is interested in individuals] free, specific, informed and unambiguous ‘**opt-in**’ consent would almost always be required, otherwise **further use cannot be considered compatible**. Importantly, such consent should be required, for example, for tracking and profiling for purposes of direct marketing, behavioural advertisement, data-brokering, location-based advertising or tracking-based digital market research”

Art. 29 WP - Opinion 03/2013 on purpose limitation (WP203)

18

19

Data minimisation

Controllers should be able to clearly explain and justify the **need** to collect and hold personal data, or consider using aggregated, anonymised or (when this provides sufficient protection) pseudonymised data for profiling.

19

20

Accuracy

The data controller must ensure the accuracy of the data created by the algorithm:

- ✓ Introducing robust measures to verify and ensure on an ongoing basis that **data re-used or obtained indirectly** is accurate and up to date;
- ✓ Being transparent about the use of personal data in the algorithm, so the **individual can correct inaccuracies** and improve the quality of the data.;
- ✓ Reviewing the **accuracy of the training data**, the input data and the algorithm because inaccuracy in each of these data sets may cause inaccuracy of the output data.
- ✓ **Data quality**, including the following components: accuracy, precision, completeness, consistency, validity and timeliness.

20

21

Storage limitation

Information must be deleted or anonymised as soon as it is no longer required for the purpose for which it was collected.

This requires an **assessment of the period** during which the data controller is allowed to retain the information because keeping personal data for too long increases the risk of inaccuracies and other issues

21

22

Accountability

Accountability


- The **controller** shall be **responsible** for and be able to **demonstrate** compliance with the data protection principles
- When using an algorithm on a data set that contains personal data, the data controller is **responsible** for, and must also be able to **demonstrate** compliance with the data protection principles

22

23

Overview

- 1 Key definitions
- 2 Data protection principles
- 3 Grounds for data processing
- 4 Information rights and automated decision making
- 5 Draft AI Regulation




TILBURG UNIVERSITY

23

24

Grounds for data processing/legal basis

- Consent
- Performance of a contract
- Compliance with a legal obligation
- Vital interests
- Public interest/official authority
- Legitimate interest



TILBURG UNIVERSITY

24

25

Grounds for data processing/legal basis

Remember

- **Consent** is **not the holy grail** - it is a last resort when other legal bases do not apply
- Stricter legal bases apply for **sensitive data** (e.g. no legitimate interest)

25

26

Example: creation of user account

Contractual necessity

- Account information is recorded: name, email, payment & shipping details

Legitimate interest

- IP address and other data are checked for for identification and fraud verification (e.g., bot detection)

Compliance with legal obligation

- Copy of purchase order is archived for accounting purposes

Consent

- To sending direct marketing emails
- Remember:
 - Do not request consent for everything (see further slides)!
 - e.g., consent may be withdrawn - then the company has to cease processing

26

27

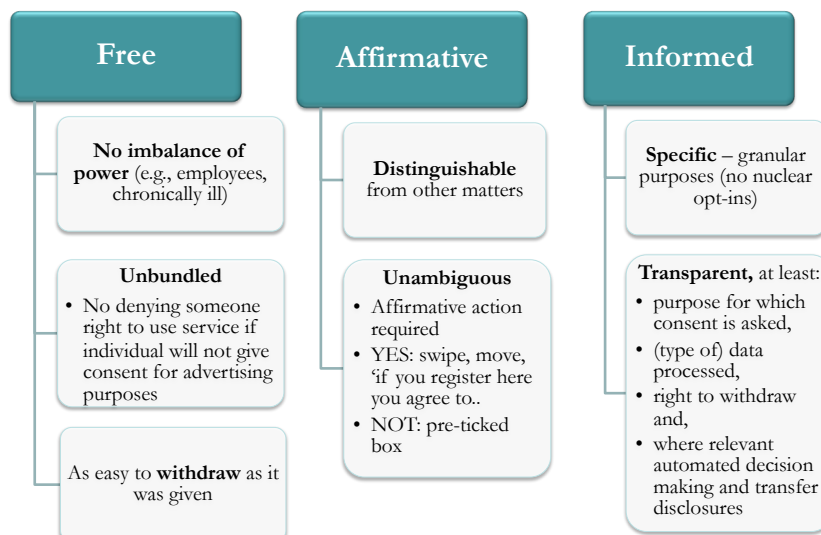
Consent

Consent 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 data relating to him or her;

27

28

Consent



28

29

Consent

- Explicit* consent for sensitive data and/or automated decision making, including profiling (see next slides)

 - Higher threshold, e.g., tick box, two-stage verification, sending an email, etc.
- Parental/legal guardian consent required for children under 16

 - However, Member States can reduce the age to 13 (e.g., France 15, Belgium 13 and UK 13)
- Consent needs to be documented

 - See also below accountability
- Remember that e-Privacy requirements may also apply

 - Cookies
 - Email direct marketing

TILBURG UNIVERSITY

29

30

Consent: examples

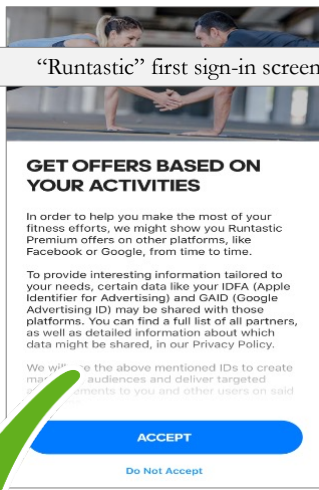
Unbundled

Do NOT make use of a running app conditional upon consent for use of:

- cross-site behavioral advertising
- combining data from other services for R&D

→ Obtain consent separately from the service

“Runtastic” first sign-in screen



GET OFFERS BASED ON YOUR ACTIVITIES

In order to help you make the most of your fitness efforts, we might show you Runtastic Premium offers on other platforms, like Facebook or Google, from time to time.

To provide interesting information tailored to your needs, certain data like your IDFA (Apple Identifier for Advertising) and GAID (Google Advertising ID) may be shared with those platforms. You can find a full list of all partners, as well as detailed information about which data might be shared, in our Privacy Policy.

We will use the above mentioned IDs to create marketing audiences and deliver targeted advertisements to you and other users on said platforms.

ACCEPT

Do Not Accept

TILBURG UNIVERSITY

30

31

Consent: examples

Distinguishable from other matters

Make consent request stand out, e.g. :

- different font, separate heading, frame
- Obtain consent outside of general statement in T&Cs or Privacy Policy

1.4 Disclaimer. Your health is very important to us. ALWAYS consult your doctor before using any product.


“Runtastic” pre sign-in language

your doctor, nor is Runtastic responsible for your behavior. The contents of the Runtastic Products, regardless whether they are provided by Runtastic, its partners or users, are not meant to supplement, let alone replace, the information provided by doctors or pharmacies. By accepting these T&C, you confirm that you are solely responsible for your health.

2 VALIDITY OF THE T&C

2.1 Validity. Runtastic offers the Runtastic Products on the basis of these T&C. The user accepts I have read and agree to the Terms & Conditions and Privacy Policy, including the processing of my health data (e.g. heart rate)

ACCEPT



TILBURG UNIVERSITY

31

32

Consent: examples

Unambiguous

Affirmative action required

- **YES:** swipe, move, ‘if you register here you agree to’
- **NO:** pre-ticked box

Pre-ticked boxes

Yes, I am over 13 years old * ?

LOGIN DETAILS

EMAIL ADDRESS *


Adidas registration

NEW PASSWORD * 👁


Please make sure your password contains a minimum of one letter, one number and is at least 8 characters long

I would like to stay up to date with adidas ?

I have read and accepted Terms & Conditions and the Adidas Privacy Statement *

I'm not a robot 

SUBMIT ➔




TILBURG UNIVERSITY

32

33

Consent is usually needed

When other GDPR grounds are not applicable or where specific rules (e.g. ePrivacy) apply	- Email direct marketing (ePrivacy)
	- Cookies (ePrivacy)
	- Sensitive data are involved (explicit consent)
	- Children's data are involved (parental consent)
	- Automated decision making (see below)
	- Profiling for commercial purposes (see below)



33

34

Sample consent language

“ Yes! Please send me tailored marketing emails about company products and services based on [prior purchases, my activities on company websites,....]. I understand that I can withdraw this consent at any time by [____].

We will handle your personal data in accordance with our privacy policy [[hyperlink to policy](#)].”




34

35

Consent and AI subsidiary

4 OCT 2021 NEWS

DeepMind Technologies Sued Over Data Sharing

 Sarah Coble News Writer

f A law firm in the United Kingdom is **suing** Google's artificial intelligence (AI) subsidiary **DeepMind Technologies** over an alleged breach of data protection laws.

t **Mishcon de Reya** is bringing a representative suit against DeepMind pertaining to the company's data-sharing deal with the Royal Free London National Health Service (NHS) Foundation Trust.

👉 A five-year partnership between the Trust and DeepMind was **announced** in 2015 to "build on the successful year-long joint project to build a smartphone app called **Streams**, which alerts clinical teams as soon as test results show that a patient is at risk of developing acute kidney injury."

The Jurist reports that "when the data-sharing agreement was made public, it was revealed that DeepMind was gaining access to a wide-ranging scope of data including admissions, discharge and transfer, accidents, emergencies, critical care, pathology and radiology data."

In July 2017, the Information Commissioner's Office (ICO) ruled the Royal Free NHS Foundation Trust failed to comply with the **Data Protection Act** when it provided patient details to DeepMind.

"The Trust provided personal data of around 1.6 million patients as part of a trial to test an alert, diagnosis and detection system for acute kidney injury," **said** the UK data protection regulator.

"But an ICO investigation found several shortcomings in how the data was handled, including that patients were not adequately informed that their data would be used as part of the test."

On September 30, Mishcon de Reya **announced** that it was bringing an action against DeepMind "on behalf of Mr Andrew Prismall and the approximately 1.6 million individuals whose confidential medical records were obtained by Google and DeepMind Technologies in breach of data protection laws."


Related to This Story

- ICO Raps NHS Trust over Protection Failure in Google Trial
- Google DeepMind Deal with NHS Contained 'Inexcusable' Mistakes
- GDPR Protection Will Continue After Google's US Data Move, Says Lawyer
- Nurse Fined After Admitting to Accessing Patient Records
- Report: NHS Doctors Sending Patient Scans via Snapchat

What's Hot on Infosecurity Magazine?

Read | Shared | Watched | Editor's Choice

1 **8 JUL 2021 NEWS**
New PrintNightmare Patch Can Be Bypassed, Say Researchers



35

36

Contract

Article 7(f) is listed as the last option among six grounds allowing for the lawful processing of personal data. It calls for a balancing test: what is necessary for the legitimate interests of the controller (or third parties) must be balanced against the interests or fundamental rights and freedoms of the data subject.


i) First, the provision covers situations where processing is **necessary** for the performance of the contract to which the data subject is a party.

ii) Second, [it] also covers processing that takes place *prior* to entering into a contract. This covers pre-contractual relations, provided that steps are taken **at the request** of the data subject, rather than at the initiative of the controller or any third party.

may also help prevent misuse of, and over-reliance on, other legal grounds.

The first five grounds of Article 7 rely on the data subject's consent, contractual arrangement, legal obligation or other specifically identified rationale as ground for legitimacy. When processing is based on one of these five grounds, it is considered as *a priori* legitimate and therefore only subject to compliance with other applicable provisions of the law. There is in

Art. 29 WP, WP217, Opinion 06/2014 on the notion of legitimate interests of the data controller



36

Contract

Controllers may wish to use profiling and automated decision-making processes because they:

- ❖ potentially allow for greater **consistency or fairness** in the decision making process (e.g. by reducing the potential for human error, discrimination and abuse of power);
- ❖ reduce the **risk of customers** failing to meet payments for goods or services (for example by using credit referencing);
or
- ❖ enable them to **deliver decisions** within a shorter time frame and improve efficiency.

Art. 29 WP - Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (WP251 rev.1)

Contract

[However,] these considerations alone are not sufficient to show that this type of processing is *necessary* under Article 6(1)(b) for the performance of a contract

The following is an example of profiling that would *not* meet the Article 6(1)(b) basis for processing.

Example

A user buys some items from an on-line retailer. In order to fulfil the contract, the retailer must process the user's credit card information for payment purposes and the user's address to deliver the goods. Completion of the contract is not dependent upon building a profile of the user's tastes and lifestyle choices based on his or her visits to the website. Even if profiling is specifically mentioned in the small print of the contract, this fact alone does not make it 'necessary' for the performance of the contract.

Art. 29 WP - Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (WP251 rev.1)

39

Legal obligation

There may be instances where there will be a legal obligation to carry out profiling – for example in connection with **fraud prevention** or **money laundering**

Art. 29 WP - Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (WP251 rev.1)

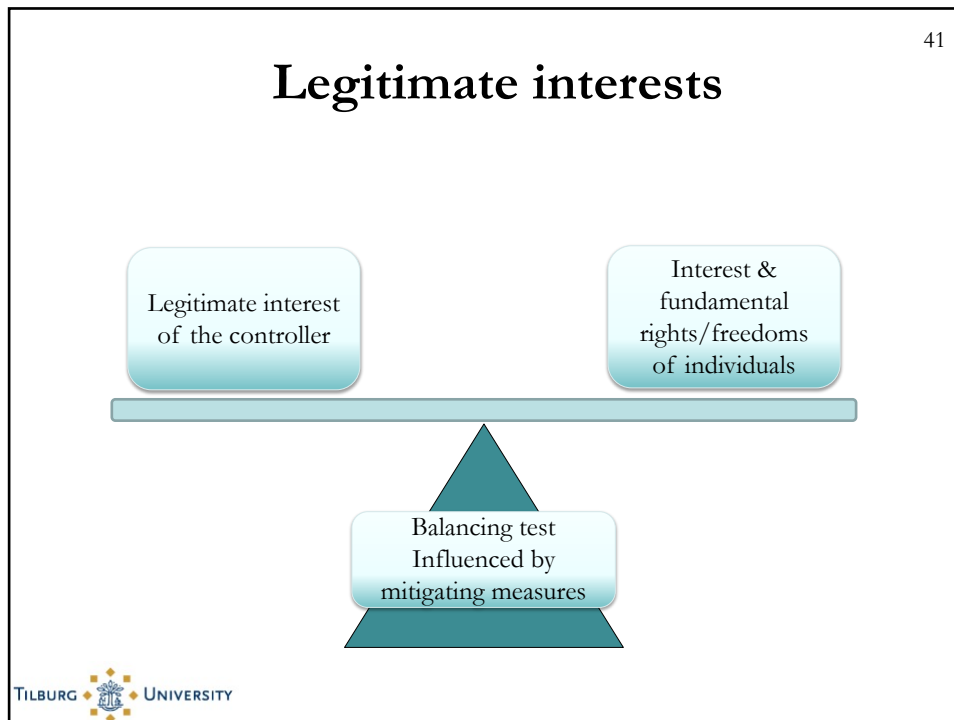
39

40

Legitimate interests

- ✓ Processing is necessary for the purposes of the **legitimate interests**
- ✓ pursued by the **controller** or by a **third party**,
- ✓ except where such interests are **overridden** by the **interests or fundamental rights and freedoms** of the data subject which require protection of personal data, in particular where the data subject is a child.

40



41

42

Legitimate interests

Article 7(f) is listed as the last option among six grounds allowing for the lawful processing of personal data. It calls for a balancing test: what is necessary for the legitimate interests of the controller (or third parties) must be balanced against the interests or fundamental rights and

An **interest** [...] is the **broader stake** that a controller may have in the processing, or the **benefit** that the controller derives -or that society might derive- from the processing. [...] Interests that are too vague or speculative will not be sufficient. [...] The notion of legitimate interest could include a broad range of interests, whether trivial or very compelling, straightforward or more controversial. It will then be in a second step, when it comes to balancing these interests against the interests and fundamental rights of the data subjects, that a more restricted approach and more substantive analysis should be taken.

processing is based on one of these five grounds, it is considered as *a priori* legitimate and therefore only subject to compliance with other applicable provisions of the law. There is in

Art. 29 WP, WP217, Opinion 06/2014 on the notion of legitimate interests of the data controller

TILBURG UNIVERSITY

42

43

Lawfulness of processing

The controller must carry out a balancing exercise to assess whether their interests are overridden by the data subject's interests or fundamental rights and freedoms. The following are particularly relevant:

- the level of **detail** of the profile
- the **comprehensiveness** of the profile;
- the **impact** of the profile; and
- the **safeguards** aimed at ensuring fairness, non-discrimination and accuracy in the profiling process.

Art. 29 WP - Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (WP251 rev.1)

43

44

Lawfulness of processing

It would be difficult for controllers to justify using legitimate interests as a lawful basis for **intrusive profiling** and **tracking practices** for marketing or advertising purposes, for example those that involve tracking individuals across multiple websites, locations, devices, services or data-brokering.


Art. 29 WP - Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (WP251 rev.1)

44

45

Overview

- 1 Key definitions
- 2 Data protection principles
- 3 Grounds for data processing
- 4 Information rights and automated decision making
- 5 Draft AI Regulation







45




46

Data subject rights


Key Rights

 Notice (Article 13/14) Individuals must receive certain information about the processing of their data	 Access (Article 15) Individuals may request access to their personal data and an explanation of personal data use	 Correction (Article 16) Individuals may request that inaccurate personal data about them are corrected	 Portability (NEW) (Article 20) Individuals may request a copy of their personal data in a standardized machine-readable format
--	---	--	--

Other Rights

 Restriction (NEW) (Article 18) Individuals may request that the controller “quarantine” their personal data , i.e., that use of information is ceased other than storing it	 Objection (Article 21) Individuals may object to controller’s use of their personal data , e.g., for direct marketing purposes	 Deletion (Article 17) Individuals may request that controller delete their personal data
---	--	--

If you get a request, forward to the DPO



46

47

Data subject rights: examples

- **Notice:** company informs consumers about the use of their personal data through its Privacy Policy
- **Access:** a consumer requests access to his/her purchase history
- **Rectification:** a supplier representative notifies you that he/she is no longer working for the supplier and requests you update his/her information
- **Portability:** a consumer requests to have his/her product customization history or running playlist sent to him/her in order to upload them to another platform for similar purposes
- **Objection:** a consumer requests to be opted-out from direct marketing based on profiling
- **Deletion:** a consumer terminates his/her user account and requests that his/her buying history and other account information be erased

47

48

Data subject rights

The data controller must ensure that it is able to process and fulfill individuals' requests, such as access, correction and objection requests, and thus

- ✓ Provide each individual with access to the categories of data that have been or will be used for the profile and information on why these are considered relevant;
- ✓ Be able to update or correct data or profiles upon the individual's request
- ✓ Be able to stop using an individual's personal data for profiling when he/she objects to this use of personal information

48

A closer look to rights relevant for ML and AI

Right of information

Information to be provided where personal data are collected from the data subject (Art. 13)

2. In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the **following further information** necessary to ensure fair and transparent processing:

(f) the **existence** of **automated decision-making**, including **profiling**, referred to in Article 22(1) and (4) and, at least in those cases, **meaningful** information about the **logic involved**, as well as the **significance** and the **envisaged consequences** of such processing for the data subject.

51

Right of information

Information to be provided where personal data have not been obtained from the data subject (Art. 14)

2. In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the **following further information** necessary to ensure fair and transparent processing in respect of the data subject:

(g) the **existence** of **automated decision-making**, including **profiling**, referred to in Article 22(1) and (4) and, at least in those cases, **meaningful** information about the **logic involved**, as well as the **significance** and the **envisaged consequences** of such processing for the data subject.



51

52

Right to an explanation

Right of access by the data subject (Art. 15)

1. The data subject shall have the **right to obtain** from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following **information**:

...

(h) the **existence** of **automated decision-making**, including **profiling**, referred to in Article 22(1) and (4) and, at least in those cases, **meaningful** information about the **logic involved**, as well as the **significance** and the **envisaged consequences** of such processing for the data subject.



52

53

Automated decision making, including profiling

Art. 22.1. 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.

53

54

Automated decision making, including profiling

“Profiling” means

- Any automated analyzing or predicting of personal aspects concerning that individual’s performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements
- Therefore any processing for business intelligence is covered

“Automated decision-making” means

- Any automated **decision** (no human intervention)
- That has **legal** or **other, similarly significant effect** on the individual
- Example: automatic rejection of loan

54

55

Profiling

Profiling is

- Not an e-privacy issue – it is regulated under the GDPR
- BUT profiling often entails cookies or can lead to direct marketing
→ Then e-privacy kicks-in
- Definition: the search for new “knowledge” about people, based on inferences that are not as such in the objective facts

Profiling is not making a database query for known facts

- Not: Looking up my address in a database
- But: Inferring that I may be a liberal because I live in a certain postal code (of which it may be known that many residents are liberals)

Profiling is the search for correlations and applying these as causality (stereotyping)

- Always history based

55


56

[The idea that] data subject [have] control over their personal data ... is in line with the fundamental principles of the GDPR. Interpreting Article 22 as **a prohibition** rather than a **right** to be invoked means that individuals are automatically protected from the potential effects this type of processing may have.

...

However the Article 22(1) prohibition only applies in specific circumstances when a decision based solely on automated processing, including profiling, has a legal effect on or similarly significantly affects someone.... Even in these cases there are defined exceptions which allow such processing to take place.

Art. 29 WP - Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (WP251 rev.1)

TILBURG  UNIVERSITY

56

57

Consent

Explicit consent is one of the exceptions for the prohibition of automated decision-making and profiling

Profiling can be opaque. Often it relies upon data that is **derived or inferred** from other data, rather than data directly provided by the data subject.

Controllers seeking to rely upon **consent** as a basis for profiling will need to show that data subjects **understand exactly** what they are consenting to and remember that consent is **not always an appropriate basis** for the processing. In all cases, data subjects should have enough relevant information about the envisaged use and consequences of profiling to ensure that any consent they provide represents an informed choice

Art. 29 WP - Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (WP251 rev.1)


57

58

Automated decisions can be based on any type of data, for example:

- data provided **directly by the individuals** concerned (such as responses to a questionnaire);
- data **observed** about the individuals (such as location data collected via an application);
- derived or inferred data** such as a profile of the individual that has already been created (e.g. a credit score).

Art. 29 WP - Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (WP251 rev.1)


 TILBURG UNIVERSITY

58

Article 22(1) refers to decisions ‘**based solely**’ on automated processing. This means that there is no human involvement in the decision process.

Example

An automated process produces what is in effect a recommendation concerning a data subject. If a human being reviews and takes account of other factors in making the final decision, that decision would not be ‘based solely’ on automated processing.

Art. 29 WP - Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (WP251 rev.1)

Decision producing legal effects

A legal effect requires that the decision, which is based on solely automated processing, affects someone’s **legal rights**, such as the freedom to associate with others, vote in an election, or take legal action. A legal effect may also be something that affects a person’s **legal status** or their **rights under a contract**. Examples of this type of effect include automated decisions about an individual that result in:

- cancellation of a contract;
- entitlement to or denial of a particular social benefit granted by law, such as child or housing benefit;
- refused admission to a country or denial of citizenship.

Art. 29 WP - Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (WP251 rev.1)

61

Similarly significantly affects him or her

For data processing to significantly affect someone the effects of the processing must be **sufficiently great or important** to be worthy of attention. In other words, the decision must have the potential to:

- significantly **affect** the circumstances, behaviour or choices of the individuals concerned;
- have a prolonged or permanent **impact** on the data subject;
- or
- at its most extreme, lead to the **exclusion or discrimination** of individuals.

Art. 29 WP - Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (WP251 rev.1)



61

62

Similarly significantly affects him or her

It is difficult to be precise about what would be considered sufficiently *significant* to meet the threshold, although the following decisions could fall into this category:

- decisions that affect someone's **financial circumstances**, such as their eligibility to credit
- decisions that affect someone's **access to health services**
- decisions that **deny** someone an employment opportunity or put them at a **serious disadvantage**
- decisions that affect someone's **access to education**, for example university admissions

Art. 29 WP - Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (WP251 rev.1)



TILT - Tilburg Institute for Law, Technology, and Society

62


63

In many typical cases the decision to present **targeted advertising** based on profiling will not have a similarly significant effect on individuals, for example an advertisement for a mainstream online fashion outlet based on a simple demographic profile: “women in the Brussels region aged between 25 and 35 who are likely to be interested in fashion and certain clothing items’

However it is **possible** that it may do, depending upon the particular characteristics of the case, including:

- the intrusiveness of the profiling process, including the tracking of individuals across different websites, devices and services;
- the expectations and wishes of the individuals concerned;
- the way the advert is delivered; or
- using knowledge of the vulnerabilities of the data subjects targeted.

Art. 29 WP - Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (WP251 rev.1)




63

64

Automated decision making, including profiling

Art. 22.2. 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**.



64

65

Automated decision making, including profiling

Art. 22.3. 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.

* (2)(a) is **necessary** for **entering into**, or **performance** of, a **contract** between the data subject and a data controller;

* (2)(c) is based on the data subject's **explicit consent**.

65

66

Suitable measures

The data controller must implement suitable measures

- ✓ Performing regular **quality assurance checks** of the algorithm to ensure that individuals are treated fairly and not unlawfully discriminated against
- ✓ Completing **algorithmic auditing** to ensure the intended performance of the algorithm and search for unlawfully discriminatory, erroneous or unjustified results
- ✓ Using **anonymisation or pseudonimisation** where possible
- ✓ Enabling the individuals to express their point of view and/or **contest the profile**

66

67

Suitable measures

The data controller must implement suitable measures

- ✓ Maintaining a mechanism for **human intervention** to provide individuals with the option to appeal, which triggers a human review
- ✓ Obtaining **certification** or following a **code of conduct** for the use of the algorithm
- ✓ Instituting an **ethical review board** to assess the algorithm's potential harms and benefits to society

67

68

Human intervention is a key element. Any review must be carried out by someone who has the appropriate authority and capability to change the decision. The reviewer should undertake a **thorough assessment** of all the relevant data, including any additional information provided by the data subject.

68

69

Automated decision making, including profiling

Art. 22.4. 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.

69

70

When is profiling for commercial purposes allowed based on the legitimate interest?

WP29 in earlier opinions:

- profiling for **Business Intelligence** generally satisfies the "compatibility requirement" and is permitted on the "legitimate interest ground", provided adequate measures to mitigate risks to privacy are implemented
- profiling for **Personalised Direct Marketing** (both via e-mail and in-site advertising)
 - does not satisfy the compatibility requirement
 - cannot be based on the legitimate interest ground
 - appears to fall within the scope of 'automated decision-making' for which the prior consent of the individual is required
- profiling for **Personalised Decision-Making** falls within the provision of automated decision-making for which the prior consent of the individual is required.

70

When is profiling for commercial purposes allowed based on the legitimate interest?

GDPR seems more lenient

- **Recital 47**: indicates expressly (and without qualification) that “the processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest.”
- **Recital 70**: indicates that “where personal data are processed for the purposes of direct marketing”, the data subject should have the right to object “**including profiling to the extent that it is related to such direct marketing**”;

When is profiling for commercial purposes allowed based on the legitimate interest?

Some conclusions:

- GDPR does appear to offer more latitude for profiling for **Personalised Direct Marketing**
- and in any event does not seem to qualify profiling for Personalised Direct Marketing under “automated decision-making”

73


Automated decision making, including profiling: in sum

Provision on “Automated individual decision-making, including profiling” (Article 22(1) GDPR)

- “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.”

Exceptions:

- The decision is necessary for entering into, or performance of, a contract between the individual and the data controller. Example: credit check
- Member State law authorizes the automated decision-making
- Explicit consent individual

 TILBURG UNIVERSITY

73

74

Automated decision making, including profiling: in sum


Strict conditions, only allowed when

- Individuals explicit consent is obtained
- Necessary to conclude or perform contract
- Authorised by EU/Member State law

Individual must be informed about the

- Existence of profiling and/or automated decision making
- Significance and consequences of the profiling and/or automated decision making
- Logic involved in the automated decision making

Individual may request human intervention, express their views, request an explanation of the decision and contest the decision


 TILBURG UNIVERSITY

74

75

Overview

- 1 Key definitions
- 2 Data protection principles
- 3 Grounds for data processing
- 4 Information rights and automated decision making
- 5 Draft AI Regulation

 TILBURG UNIVERSITY

75

76

EC Proposal for AI Regulation



EUROPEAN
COMMISSION

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**

{SEC(2021) 167 final} - {SWD(2021) 84 final} - {SWD(2021) 85 final}

 TILBURG UNIVERSITY

76

77

Relation to data protection

The proposal is **without prejudice** and **complements** the General Data Protection Regulation (Regulation (EU) 2016/679) and the Law Enforcement Directive (Directive (EU) 2016/680) with a set of harmonised **rules** applicable to the design, development and use of certain high-risk AI systems and **restrictions** on certain uses of remote biometric identification systems.

Explanatory memorandum EC Proposal AI Regulation



77

78

EC Proposal for AI Regulation

Risk based regulation

High-risk AI systems and non-high risk



different requirements depending on the level of risk



78

79

Subject matter

- (a) harmonised rules for the placing on the market, the putting into service and the use of artificial intelligence systems ('AI systems') in the Union;
- (a) **prohibitions** of certain artificial intelligence practices;
- (b) specific **requirements for high-risk AI systems** and obligations for operators of such systems;

Art. 1 EC Proposal AI Regulation

79

80

Subject matter

- (c) harmonised **transparency rules for AI systems** intended to interact with natural persons, **emotion recognition systems** and **biometric categorisation systems**, and **AI systems used to generate or manipulate image, audio or video content**;
- (d) rules on market monitoring and surveillance.

Art. 1 EC Proposal AI Regulation

80

81

Scope

This Regulation applies to:

- (a) **providers placing** on the market or **putting into service** AI systems in the Union, irrespective of whether those providers are established within the Union or in a third country;
- (b) **users** of AI systems located within the Union;
- (c) **providers and users** of AI systems that are located in a third country, where the **output** produced by the system **is used** in the Union;

Art. 2(1) EC Proposal AI Regulation

81

82

Scope

This Regulation applies to:

- 2. For high-risk AI systems that are safety components of products or systems, or which are themselves products or systems, falling within the scope of the following acts, only Article 84 of this Regulation shall apply:
 - (a) Regulation (EC) 300/2008;
 - (b) Regulation (EU) No 167/2013;
 - (c) Regulation (EU) No 168/2013;
 - (d) Directive 2014/90/EU;
 - (e) Directive (EU) 2016/797;
 - (f) Regulation (EU) 2018/858;
 - (g) Regulation (EU) 2018/1139;
 - (h) Regulation (EU) 2019/2144.

Art. 2(1) EC Proposal AI Regulation

82

Scope

This Regulation applies to:

3. This Regulation shall **not** apply to AI systems developed or used exclusively for **military purposes**.

4. This Regulation shall **not** apply to **public authorities in a third country** nor to **international organisations** falling within the scope of this Regulation pursuant to paragraph 1, where those authorities or organisations use AI systems in the framework of international agreements for law enforcement and judicial cooperation with the Union or with one or more Member States.

5. This Regulation shall **not** affect the application of the provisions on the **liability of intermediary service providers** set out in Chapter II, Section IV of Directive 2000/31/EC of the European Parliament and of the Council 60 [as to be replaced by the corresponding provisions of the Digital Services Act].

Art. 2 EC Proposal AI Regulation

Definitions

“**artificial intelligence system**’ (AI system) means **software** that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, **generate outputs such as content, predictions, recommendations, or decisions influencing** the environments they interact with”

Art. 3(1) EC Proposal AI Regulation

Annex I

ANNEX I

ARTIFICIAL INTELLIGENCE TECHNIQUES AND APPROACHES referred to in Article 3, point 1

- (a) Machine learning approaches, including supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning;
- (b) Logic- and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning and expert systems;
- (c) Statistical approaches, Bayesian estimation, search and optimization methods.

Definitions

- (34) ‘emotion **recognition** system’ means an AI system for the purpose of **identifying or inferring emotions or intentions** of natural persons on the basis of their biometric data;
- (35) ‘biometric **categorisation** system’ means an AI system **for the purpose of assigning natural persons to specific categories**, such as sex, age, hair colour, eye colour, tattoos, ethnic origin or sexual or political orientation, on the basis of their biometric data;

87

Definitions

- (36) ‘**remote biometric identification system**’ means an AI system for the purpose of identifying natural persons at a distance through the comparison of a person’s biometric data with the biometric data contained in a reference database, and without prior knowledge of the user of the AI system whether the person will be present and can be identified ;

Art. 3 EC Proposal AI Regulation

87

88

Definitions

- (37) “**real-time**’ remote biometric identification system’ means a remote biometric identification system whereby the capturing of biometric data, the comparison and the identification all occur without a significant delay. This comprises not only instant identification, but also limited short delays in order to avoid circumvention.
- (38) “**post**’ remote biometric identification system’ means a remote biometric identification system other than a ‘real-time’ remote biometric identification system;

Art. 3 EC Proposal AI Regulation

88

89

Prohibited AI practices

Discrimination and **manipulation** at the heart of prohibited practices

- ❑ Four prohibited AI practices

What are practices? Not defined. It seems to mean:

- “the placing on the market, putting into service or use of an AI system” that affects natural persons (first three practices) or “the use of specific AI systems” (fourth practice)

89

90

Prohibited AI practices

- ❑ 1st prohibited practice:

the placing on the market, putting into service or use of an AI system that deploys **subliminal techniques beyond a person's consciousness in order to materially distort a person's behaviour** in a manner that causes or is likely to cause that person or another person physical or psychological harm

90

91

Prohibited AI practices

❑ 2nd prohibited practice:

the placing on the market, putting into service or use of an AI system that **exploits any of the vulnerabilities of a specific group of persons due to their age, physical or mental disability**, in order to materially distort the behaviour of a person pertaining to that group in a manner that causes or is likely to cause that person or another person physical or psychological harm

91

92

Prohibited AI practices

❑ 3rd prohibited practice:

the placing on the market, putting into service or use of AI systems **by public authorities or on their behalf** for the evaluation or classification of the trustworthiness of natural persons over a certain period of time based on their social behaviour or known or predicted personal or personality characteristics, with the social score leading to either or both of the following:

- (i) detrimental or unfavourable treatment of certain natural persons or whole groups thereof in social contexts which are unrelated to the contexts in which the data was originally generated or collected;
- (ii) detrimental or unfavourable treatment of certain natural persons or whole groups thereof that is unjustified or disproportionate to their social behaviour or its gravity;

92

93

Prohibited AI practices

❑ 4th prohibited practice:

the use of ‘**real-time**’ **remote biometric identification** systems* in publicly accessible spaces for the purpose of **law enforcement**

Exceptions:

- (i) the **targeted search** for specific potential victims of crime, including missing children;
- (ii) the prevention of a specific, substantial and imminent **threat to the life or physical safety** of natural persons or of a **terrorist attack**;
- (iii) the detection, localisation, identification or prosecution of a **perpetrator or suspect of a criminal offence**.

93

94

Prohibited AI practices

❑ ‘**remote biometric identification system**’

means an AI system for the **purpose** of **identifying** natural persons **at a distance** through the **comparison** of a person’s **biometric data** with the biometric data contained in a reference database, and **without prior knowledge** of the user of the AI system whether the person will be present and can be identified . Art. 3(36) EC Proposal AI Regulation

❑ ‘**real-time**’ **remote biometric identification** system

means a **remote biometric identification system** whereby the capturing of biometric data, the comparison and the identification all occur **without a significant delay**. This comprises not only instant identification, but also limited short delays in order to avoid circumvention. Art. 3(37) EC Proposal AI Regulation

94

95

Prohibited practices

Step toe THE EU ARTIFICIAL INTELLIGENCE ACT **1**

PROHIBITED USES

The Regulation identifies a series of AI practices that are prohibited because they go against the EU values or because they violate EU individuals' fundamental rights.

The use of "real-time" remote biometric identification systems (such as facial recognition) in public spaces for law enforcement purposes will however be authorized if strictly necessary for:

1 targeted search for victims	2 prevention of specific, substantial and imminent threats or terrorist attacks	3 detection, localization, identification or prosecution of a perpetrator or suspect of certain criminal offences
----------------------------------	--	--

www.steptoe.com

Source: Steptoe

TILBURG UNIVERSITY

95

96

High risk AI systems

High risk AI systems (cumulative conditions):

- a. the AI system is **intended** to be used as a safety component of a product, or is itself a product, covered by the Union harmonisation legislation listed in Annex II;
- b. the product whose safety component is the AI system, or the AI system itself as a product, is required to undergo a **third-party conformity assessment** with a view to the placing on the market or putting into service of that product pursuant to the Union harmonisation legislation listed in Annex II

Art. 6(1) EC Proposal AI Regulation

TILBURG UNIVERSITY

96

High risk AI systems

ANNEX II

LIST OF UNION HARMONISATION LEGISLATION

Section A – List of Union harmonisation legislation based on the New Legislative Framework

1. Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC (OJ L 157, 9.6.2006, p. 24) [as repealed by the Machinery Regulation];
2. Directive 2009/48/EC of the European Parliament and of the Council of 18 June 2009 on the safety of toys (OJ L 170, 30.6.2009, p. 1);
3. Directive 2013/53/EU of the European Parliament and of the Council of 20 November 2013 on recreational craft and personal watercraft and repealing Directive 94/25/EC (OJ L 354, 28.12.2013, p. 90);
4. Directive 2014/33/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to lifts and safety components for lifts (OJ L 96, 29.3.2014, p. 251);
5. Directive 2014/34/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to equipment and protective systems intended for use in potentially explosive atmospheres (OJ L 96, 29.3.2014, p. 309);
6. Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC (OJ L 153, 22.5.2014, p. 62);
7. Directive 2014/68/EU of the European Parliament and of the Council of 15 May 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of pressure equipment (OJ L 189, 27.6.2014, p. 164);
8. Regulation (EU) 2016/424 of the European Parliament and of the Council of 9 March 2016 on cableway installations and repealing Directive 2000/9/EC (OJ L 81, 31.3.2016, p. 1);
9. Regulation (EU) 2016/425 of the European Parliament and of the Council of 9 March 2016 on personal protective equipment and repealing Council Directive 89/686/EEC (OJ L 81, 31.3.2016, p. 51);
10. Regulation (EU) 2016/426 of the European Parliament and of the Council of 9 March 2016 on appliances burning gaseous fuels and repealing Directive 2009/142/EC (OJ L 81, 31.3.2016, p. 99);



High risk AI systems

11. Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (OJ L 117, 5.5.2017, p. 1);
12. Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU (OJ L 117, 5.5.2017, p. 176).

Section B. List of other Union harmonisation legislation

1. Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002 (OJ L 97, 9.4.2008, p. 72).
2. Regulation (EU) No 168/2013 of the European Parliament and of the Council of 15 January 2013 on the approval and market surveillance of two- or three-wheel vehicles and quadricycles (OJ L 60, 2.3.2013, p. 52);
3. Regulation (EU) No 167/2013 of the European Parliament and of the Council of 5 February 2013 on the approval and market surveillance of agricultural and forestry vehicles (OJ L 60, 2.3.2013, p. 1);
4. Directive 2014/90/EU of the European Parliament and of the Council of 23 July 2014 on marine equipment and repealing Council Directive 96/98/EC (OJ L 257, 28.8.2014, p. 146);
5. Directive (EU) 2016/797 of the European Parliament and of the Council of 11 May 2016 on the interoperability of the rail system within the European Union (OJ L 138, 26.5.2016, p. 44).



High risk AI systems

6. Regulation (EU) 2018/858 of the European Parliament and of the Council of 30 May 2018 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles, amending Regulations (EC) No 715/2007 and (EC) No 595/2009 and repealing Directive 2007/46/EC (OJ L 151, 14.6.2018, p. 1); 3. Regulation (EU) 2019/2144 of the European Parliament and of the Council of 27 November 2019 on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users, amending Regulation (EU) 2018/858 of the European Parliament and of the Council and repealing Regulations (EC) No 78/2009, (EC) No 79/2009 and (EC) No 661/2009 of the European Parliament and of the Council and Commission Regulations (EC) No 631/2009, (EU) No 406/2010, (EU) No 672/2010, (EU) No 1003/2010, (EU) No 1005/2010, (EU) No 1008/2010, (EU) No 1009/2010, (EU) No 19/2011, (EU) No 109/2011, (EU) No 458/2011, (EU) No 65/2012, (EU) No 130/2012, (EU) No 347/2012, (EU) No 351/2012, (EU) No 1230/2012 and (EU) 2015/166 (OJ L 325, 16.12.2019, p. 1);
7. Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91 (OJ L 212, 22.8.2018, p. 1), in so far as the design, production and placing on the market of aircrafts referred to in points (a) and (b) of Article 2(1) thereof, where it concerns unmanned aircraft and their engines, propellers, parts and equipment to control them remotely, are concerned.

High risk AI systems

High risk AI systems :

In addition to the high-risk AI systems referred to in paragraph 1, AI systems referred to in Annex III shall also be considered high-risk.

High risk AI systems

ANNEX III HIGH-RISK AI SYSTEMS REFERRED TO IN ARTICLE 6(2)

High-risk AI systems pursuant to Article 6(2) are the AI systems listed in any of the following areas:

1. Biometric identification and categorisation of natural persons:
 - (a) AI systems intended to be used for the 'real-time' and 'post' remote biometric identification of natural persons;
2. Management and operation of critical infrastructure:
 - (a) AI systems intended to be used as safety components in the management and operation of road traffic and the supply of water, gas, heating and electricity.
3. Education and vocational training:
 - (a) AI systems intended to be used for the purpose of determining access or assigning natural persons to educational and vocational training institutions;
 - (b) AI systems intended to be used for the purpose of assessing students in educational and vocational training institutions and for assessing participants in tests commonly required for admission to educational institutions.
4. Employment, workers management and access to self-employment:
 - (a) AI systems intended to be used for recruitment or selection of natural persons, notably for advertising vacancies, screening or filtering applications, evaluating candidates in the course of interviews or tests;
 - (b) AI intended to be used for making decisions on promotion and termination of work-related contractual relationships, for task allocation and for monitoring and evaluating performance and behavior of persons in such relationships.



High risk AI systems

5. Access to and enjoyment of essential private services and public services and benefits:
 - (a) AI systems intended to be used by public authorities or on behalf of public authorities to evaluate the eligibility of natural persons for public assistance benefits and services, as well as to grant, reduce, revoke, or reclaim such benefits and services;
 - (b) AI systems intended to be used to evaluate the creditworthiness of natural persons or establish their credit score, with the exception of AI systems put into service by small scale providers for their own use;
 - (c) AI systems intended to be used to dispatch, or to establish priority in the dispatching of emergency first response services, including by firefighters and medical aid.
6. Law enforcement:
 - (a) AI systems intended to be used by law enforcement authorities for making individual risk assessments of natural persons in order to assess the risk of a natural person for offending or reoffending or the risk for potential victims of criminal offences;
 - (b) AI systems intended to be used by law enforcement authorities as polygraphs and similar tools or to detect the emotional state of a natural person;
 - (c) AI systems intended to be used by law enforcement authorities to detect deep fakes as referred to in article 52(3);
 - (d) AI systems intended to be used by law enforcement authorities for evaluation of the reliability of evidence in the course of investigation or prosecution of criminal offences;
 - (e) AI systems intended to be used by law enforcement authorities for predicting the occurrence or reoccurrence of an actual or potential criminal offence based on profiling of natural persons as referred to in Article 3(4) of Directive (EU) 2016/680 or assessing personality traits and characteristics or past criminal behaviour of natural persons or groups;
 - (f) AI systems intended to be used by law enforcement authorities for profiling of natural persons as referred to in Article 3(4) of Directive (EU) 2016/680 in the course of detection, investigation or prosecution of criminal offences;
 - (g) AI systems intended to be used for crime analytics regarding natural persons, allowing law enforcement authorities to search complex related and unrelated large data sets available in different data sources or in different data formats in order to identify unknown patterns or discover hidden relationships in the data.



High risk AI systems

7. Migration, asylum and border control management:
 - (a) AI systems intended to be used by competent public authorities as polygraphs and similar tools or to detect the emotional state of a natural person;
 - (b) AI systems intended to be used by competent public authorities to assess a risk, including a security risk, a risk of irregular immigration, or a health risk, posed by a natural person who intends to enter or has entered into the territory of a Member State;
 - (c) AI systems intended to be used by competent public authorities for the verification of the authenticity of travel documents and supporting documentation of natural persons and detect non-authentic documents by checking their security features;
 - (d) AI systems intended to assist competent public authorities for the examination of applications for asylum, visa and residence permits and associated complaints with regard to the eligibility of the natural persons applying for a status.
8. Administration of justice and democratic processes:
 - (a) AI systems intended to assist a judicial authority in researching and interpreting facts and the law and in applying the law to a concrete set of facts.

Requirements for high risk AI systems before they enter the market


- Risk management system (Art.9)
 - Risk identification
 - Risk evaluation
 - Adoption of risk management measures
 - Mandatory testing to identify the most suitable risk management measure.
- Data governance: Training, validation and testing **data sets** shall be relevant, representative, free of errors and complete. (Art. 10)

105

Requirements for high risk AI systems before they enter the market

- ❑ Technical documentation (Art.11) and record keeping (Art. 12) obligations
 - Automatic recording of events (logging) to **ensure traceability of the AI system's functioning is appropriate to the intended purpose**. Example of data: input data that led to a match.
- ❑ Human oversight measures (Art. 14)
- ❑ Accuracy & Cybersecurity obligations (Art. 15)
- ❑ Transparency obligations (Art. 13)

EC Proposal AI Regulation







105

106


EC Proposal for AI Regulation

New rules for providers of high-risk AI systems

Step 1	Step 2	Step 3	Step 4
			
A high-risk AI system is developed	It needs to undergo the conformity assessment and comply with AI requirements For some systems a notified body is involved	Registration of stand-alone AI systems in an EU database	A declaration of conformity needs to be signed and the AI system should bear the CE marking. The system can be placed on the market <i>If substantial changes happen in the AI system's lifecycle, go back to Step 2</i>

Once the AI system is on the market, authorities are in charge of the market surveillance, users ensure human oversight and monitoring, while providers have a post-market monitoring system in place. Providers and users will also report serious incidents and malfunctioning.

Antonella Zara



106

107

Human oversight measures

1. High-risk AI systems shall be designed and developed in such a way, including with appropriate human-machine interface tools, that they can be effectively overseen by natural persons during the period in which the AI system is in use.
2. Human oversight shall aim at preventing or minimising the risks to health, safety or fundamental rights that may emerge when a high-risk AI system is used in accordance with its intended purpose or under conditions of reasonably foreseeable misuse, in particular when such risks persist notwithstanding the application of other requirements set out in this Chapter. [...]

107

108

Human oversight measures

However, due to the strong potential impact of certain AI systems for individuals or groups of individuals, **real human centrality** should leverage on highly qualified human oversight and a lawful processing as far as such systems are based on the processing of personal data or process personal data to fulfil their task so as to ensure that **the right not to be subject to a decision based solely on automated processing is respected.**

108

109

Requirements for different actors

- Obligations for providers (developers)
- Obligations for users (Art. 29): use in line with instructions and intended purpose & if they suspect a risk, they must suspend the system and notify providers.
- Obligations for importers
- Obligations for distributors

109

110

Regulatory oversight

- Oversight and enforcement
- National supervisory authorities and a new European Artificial Intelligence Board
- Penalties up to 30m EUR for non-compliance with the requirements of the AI Regulation.


110

111

Conformity assessment

The AIA proposal foresees a procedure for
conformity assessment

Art. 43 EC Proposal AI Regulation



TILBURG UNIVERSITY


111

112

Conformity assessment

- Following the example of ‘New Approach’ legislation (e.g. medical devices): assessment by accredited third party or self-assessment and CE Marking.
- Harmonised European standards will be developed by the European standardisation organisations (CEN, CENELEC, ETSI) to cover the requirements of the Regulation.

EC Proposal AI Regulation



TILBURG UNIVERSITY

112

Conformity assessment

the EDPB and the EDPS advocate adapting the conformity assessment procedure under Article 43 of the Proposal to the effect that an ex ante third-party conformity assessment must generally be carried out for high-risk AI. Although a third-party conformity assessment for high-risk processing of personal data is not a requirement in the GDPR or EUDPR, the risks posed by AI systems are yet to be fully understood. The general inclusion of an obligation for third-party conformity assessment would therefore further strengthen legal certainty and confidence in all high-risk AI systems.

Thank you for your attention!

Prof. Dr. Eleni KOSTA
e.kosta@tilburguniversity.edu

Professor of Technology Law and Human Rights
Tilburg Institute for Law, Technology, and Society (TILT)
Tilburg University