Tech Me Up!

AI webinar series

by TaylorWessing

Session #4

AI, lawful bases, transparency and fairness: how to thread the GDPR needle

Mareike Gehrmann, Fabrizio Sanna, Chris Jeffery, Benjamin Znaty.

Host: Paul Voigt

12 September 2023

Contents

Tech Me Up!
AI webinar series
by TaylorWessing

#1 Intro – how and where is privacy relevant regarding AI, training on PII, use of PII

Approach of the analysis:

Tech Me Up! AI webinar series by TaylorWessing

APPLICATION OF PRIVACY RULES AND OBLIGATION TO AI PROVIDERS

USE OF AI TO FACILITATE COMPLIANCE WITH PRIVACY RULES AND OBLIGATIONS

Tech Me Up!
AI webinar series
by TaylorWessing

#2 AI and legal basis for processing

Processing by the AI provider and legal basis

Tech Me Up! AI webinar series by TaylorWessing

Contract

- Processing necessary to perform a task assigned by the users
- Requires taking into account (i) nature of the service; (ii) whether the service can be provided without the processing

Consent / Legitimate interest

Processing carried out in the interest of the AI provider

- General GDPR consent requirements apply
- DPIA showing necessity and proportionality of the processing

Choice among the two, especially as regards machine learning, deeply influenced by the approach adopted in future AI regulation which will need to strike a balance between interest in AI development and privacy

Legal obligation

- AI system used to ensure its compliance with legislation must be specifically identified
- Legislation triggering the processing must be specifically identified

Public interest

- AI is used as part of the exercise of official authority, or to perform a task in the public interest set out by law

Vital interest

- Limited application only, e.g. for emergency medical diagnosis of patients who are otherwise incapable of providing consent

Using AI to comply with legal basis requirements

AI may be used to make a granular and more precise selection of the legal basis, especially if integrated with the tools used for the processing and trained with the processing background (especially the purposes). E.g.:

Ai may be used to map contracts, their changes and termination assuring correspondence between contractual dispositions and processing

regarding consent, AI may be used to collect and map user consent

regarding legitimate interest AI may serve as a support to elaborate DPIAs

Tech Me Up!
AI webinar series
by TaylorWessing

#3 Data Processing Agreements (DPAs)

Data Processing Agreements

Tech Me Up! AI webinar series by TaylorWessing

AI providers and DPA obligations

Data processor v data controller

- AI is an instrument used by a third-party controller of the data
  - AI provider to arrange and make available standardized and non-negotiable DPAs
- AI provider processes the data in its interest as controller
  - obligation (at least) to provide interested party with privacy policy describing the processing and identifying the legal basis used
- The two approaches may be combined in relation to the different processing that are carried out through the use of the AI
- At benchmark level the main AI provider are classified as ‘controllers’ (Midjourney, ChatGTP, Siri, Alexa, Bard)

Using AI in DPA creation

- AI may map the processing and the inputs based on which they are carried out determining roles and identifying adequate security measures
- AI may support in the creation of DPA based on the information provided by the controller on which behalf the DPA
- The AI may pre-set limits on the use of the data based on the DPA
- There are aspects that require human supervision entailing discretionary determinations

Tech Me Up!
AI webinar series
by TaylorWessing

#4 Transparency and data subject rights, Art. 12 to 21 GDPR

(Art. 22 GDPR excluded)

Transparency and data subject rights – overview

Tech Me Up! AI webinar series by TaylorWessing

Art. 12: **Transparent information, communication and modalities for the exercise** of the rights of the data subject

Art. 13: **Information** to be provided where personal data are collected from the data subject

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

Art. 15: Right of **access** by the data subject

Art. 16: Right to **rectification**

Art. 17: Right to **erasure ('right to be forgotten')**

Art. 18: Right to **restriction of processing**

Art. 19: **Notification** obligation regarding rectification or erasure of personal data or restriction of processing

Art. 20: Right to **data portability**

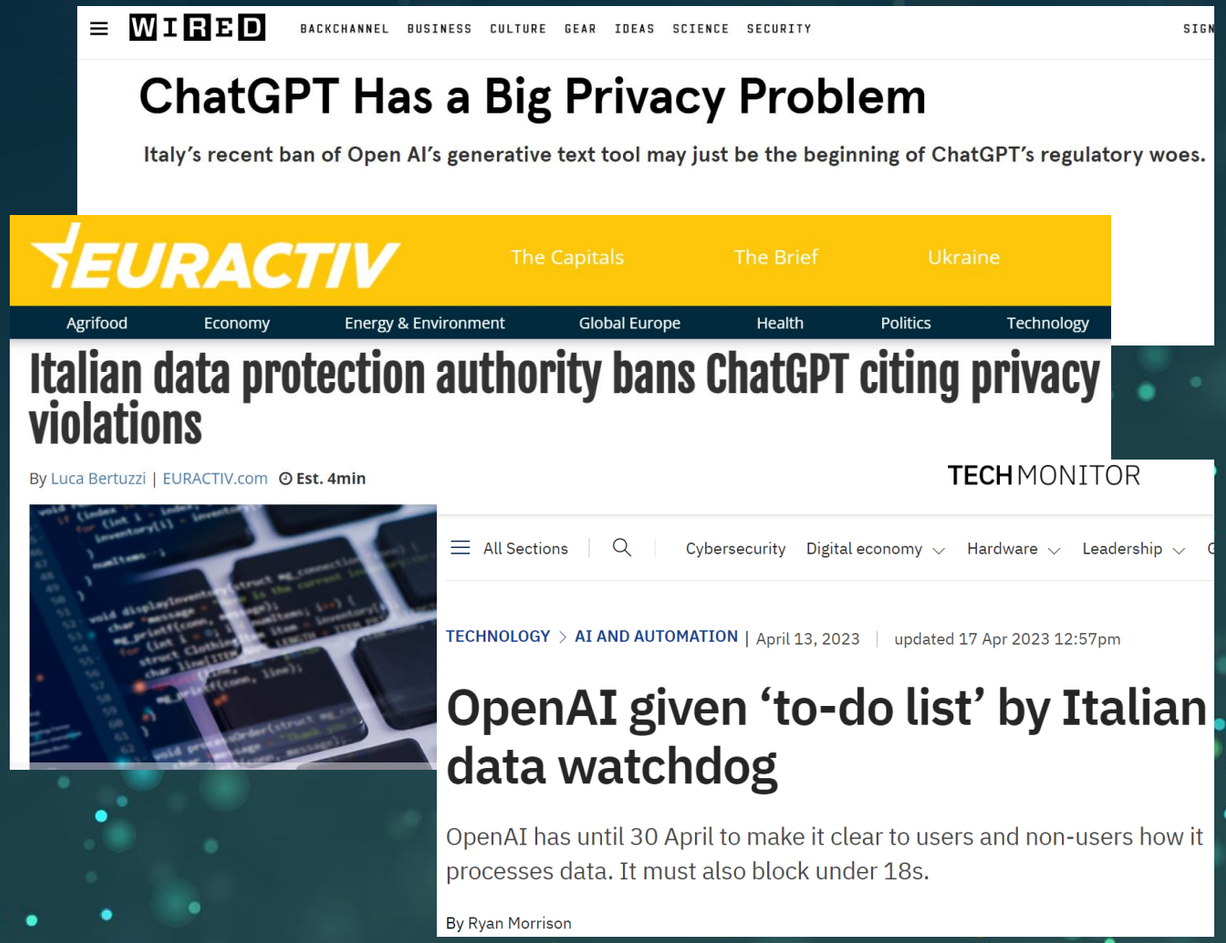
Art. 21: Right to **object**

To be ensured by controller:

Who is the controller? Different purposes, different roles, different duties!

Privacy Challenges – Example "ChatGPT"

- Among other **privacy concerns**, it is suspected that OpenAI did not sufficiently guarantee **data subject rights**
- In particular:
  - People whose data is **collected** by OpenAI are not adequately **informed** about this data processing
  - No information about **data sources**
  - No information about the **algorithms** behind the automated data processing
  - No mechanisms for data subjects (users and non-users) to request **rectification and erasure**, and to **object** to processing
  - No clarity on whether data is **shared with third parties** with commercial interests
  - **Enable** data subject rights, such as information and deletion, **even for non-users**



How to overcome the challenges?

Risk reduction to zero does not exist!

- Initial question: Should the users be allowed to enter personal data?
  - Yes: Not sufficient to merely refer to AI provider's privacy policy
- Next check: Are there third party data processing activities?
  - Use of personal data for training purposes?
  - Option, to switch off?
- Next check: Identification of my
  - own data processing activities
  - own roles
  - own duties

Transparency:

- Information about all data processing activities: (i) original learning of the AI, (ii) user input, (iii) further learning of the AI
- Challenges: Meaningful information about
  - the use of personal data for training (decision process is a "blackbox")
  - the logic involved [of AI] and the scope and intended effects of such processing for the data subject (Art. 22 GDPR)
- CNIL mentions facilitation in handout: Orientation? Please document when such statements are the basis for use.

Data subject rights, two examples:

- Further data subject rights, two examples:
  - Art. 17: Deletion of personal training data is hardly possible, so reduce the risk by data minimization
  - Art. 15: Right to access is restricted – but cannot be denied – if it would disclose trade secrets (see recital 63), (no) detailed information about the logic of the AI? As AI deployer ask the AI provider for documentation!
- 100 % fulfillment of data subject rights is not possible, therefore reduce the risk by measures, assess the risks and make an informed decision

Tech Me Up!
AI webinar series
by TaylorWessing

#6 Security & Privacy by Design and Default

Security & Privacy by Design and Default
Main concerns and solutions

Tech Me Up! AI webinar series by TaylorWessing

Data Minimisation vs Statistical Accuracy

Sequencing the processing (Training vs Production)

Heavy reliance on API and third parties

Privacy and Security from Day 1

New vulnerabilities & threats specific to AI (Poisoning, Inference, Evasion and Extraction)

Establishing approved services/sources (data, model, code)

Updating and improving existing security policies:
At the training phase (Federate Learning, Synthetic Data, Adding noise)
At the production phase (Encryption & Conversion, Localized use, Privacy-preserving approaches, Anonymisation)

Risks related to prompts and use (e.g. Samsung Leak)

Implementing organizational policies for AI

Generative AI used for cyber attacks

DPIAs and other types of risks assessments

Tech Me Up!
AI webinar series
by TaylorWessing

#5 Art. 22 GDPR and other GDPR requirements to be observed

Automated decision-making

- AI lends itself to ADM
- Discrimination risk
- What is ADM?
- Scope not as clear as you might think – Schufa CJEU.
- Don't assume that because there is some human intervention, there is no ADM.
- What's the big deal?
- Not a right to object – effectively separate lawful bases for ADM, so don't assume LI will work!
- ICO recommendations;
- Info re processing – incl weaknesses in the logic
- Simple ways to request human intervention
- Regular checks to ensure system working

- Art 22 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:
  - Necessary for a contract with the individual
  - Authorised by EU law
  - Explicit consent
- Safeguard user rights and freedoms AT LEAST right to human intervention and right to contest the decision

UK approach to AI & privacy

- ICO detailed but practical guidance
- Transparency guidance with Alan Turing institute
- 140 pages of guidance on applying GDPR generally to machine-learning AI
- Risk-based, practical (if voluminous) guide to applying fairness & lawfulness, transparency, controller-processor categorisation, purpose limitation, accountability, data subject rights
- A mix of "you must do this" and good practice recommendations
- AI risk toolkit under consultation

Tech Me Up!
AI webinar series
by TaylorWessing

Q&A

Speakers

Tech Me Up!
AI webinar series
by TaylorWessing

Mareike Gehrmann
Partner,
Taylor Wessing

Christopher Jeffery
Partner,
Taylor Wessing

Fabrizio Sanna
Partner,
Orsingher Ortu

Benjamin Znaty
Counsel,
Taylor Wessing

Dr. Paul Voigt
Partner,
Taylor Wessing

taylorwessing.com