# What do we do when AI and Data Science gets up to no good?

Dr Susheel Varma FBCS – Head of AI & Data Science, ICO

2022-10-11 – AI & Data4Good Workshop
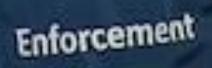
ico.org.uk

# Clearview AI

- ## Enforcement Notice (Summary)

  1. Delete any personal data of data subjects resident in the UK that is held in the Clearview Database.

  2. Refrain from any further processing of the personal data of data subjects resident in the UK. (a) Cease obtaining or "scraping" any personal data about UK residents from the public facing internet; (b) Refrain from adding personal data about UK residents to the Clearview Database; and (c) Refrain from processing any Probe Images of UK residents, and in particular refrain from seeking to match such images against the Clearview Database.

  3. Refrain from offering any service provided by way of the Clearview Database to any customer in the UK.

  4. Not do anything in future that would come within paragraphs 1-3 above without first: (a) carrying out a DPIA compliant with Article 35 35 UK GDPR, and (b) providing a copy of that DPIA to the Commissioner

- ## Monetary Penalty Notice

  - £7,552,800 (equivalent to €9 million)

  - The Commissioner's Regulatory Action Policy (RAP) states that novel or invasive technology causing a high degree of intrusion into the privacy of individuals can expect regulatory action at the "upper end of the scale".

# ICO Notices (Enforcement, Penalty, Decision)



**ico.**
Information Commissioner's Office

The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

Home | Your data matters | For organisations | Make a complaint | **Action we've taken** | About

Action we've taken / Enforcement

## Enforcement action

**Filters**

**Type**

☑ All
☐ Monetary penalties — 66
☐ Enforcement notices — 35
☐ Prosecutions — 1

**Sector**

☑ All
☐ Retail and manufacture — 24
☐ Finance insurance and credit — 23
☐ Marketing — 23
☐ General business — 5
☐ Land or property services — 5
☐ Transport and leisure — 4
☐ Charitable and — 3

**102 in total**

**Easylife Limited**
06 October 2022, Enforcement notices, Retail and manufacture
Between 1 August 2019 and 19 August 2020, Easylife

**Easylife Limited**
05 October 2022, Monetary penalties, Retail and manufacture
Easylife Limited has contravened Article 5(1)(a) of the

**Green Logic UK Ltd**
03 October 2022, Monetary penalties, Retail and manufacture
Between 1 January 2020 and 31 December 2020, Gree

**Eco Spray Insulations Limited**
03 October 2022, Monetary penalties, Retail and manufacture
Between 2 January 2020 and 30 September 2020, Eco

**Euroseal Windows Limited**
03 October 2022, Enforcement notices, Retail and manufacture
Between 1 January 2020 and 2 December 2020, Eurose

---

**ico.**
Information Commissioner's Office

The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

Home | Your data matters | For organisations | Make a complaint | Action we've taken | About the ICO

Action we've taken /

## Decision notices

**Filters**

**By case reference or keyword**

🔍

**By ICO decision** ❓

☐ Complaint not upheld — 10,800
☐ Complaint upheld — 8,628
☐ Complaint partly upheld — 966

**By date**

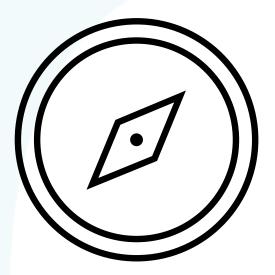○ Past month — 81
○ Past year — 1,568
○ From

dd/mm/yyyy 📅

To

dd/mm/yyyy 📅

**Showing 1 to 25 of 17,334**    Sort by  New

**Office for Standards in Education, Children's Services and Skil**
28 Sep 2022, Other

The complainant requested a copy of comments made on Parentview month period in relation to an Ofsted inspection at a named school. section 40(2) of FOIA (third party personal data) to withhold the info Commissioner's decision is that Ofsted is only entitled to rely on sec to withhold some of the information falling within the scope of the re Furthermore, that the information relating directly to the requester i disclosure under section 40(1) of FOIA. The Commissioner requires following steps: Disclose to the complainant the information in blue Annex.

FOI 40(1): Complaint not upheld    FOI 40(2): Complaint partly upheld

📄 Decision notice IC-164729-R4L3
PDF (1k)

**Clavering Parish Council**
28 Sep 2022, Local government

The complainant requested information from Clavering Parish Counc relating to legal advice sought by the Council and provided by a Barr

# Routes and practicalities of investigations

- Statutory
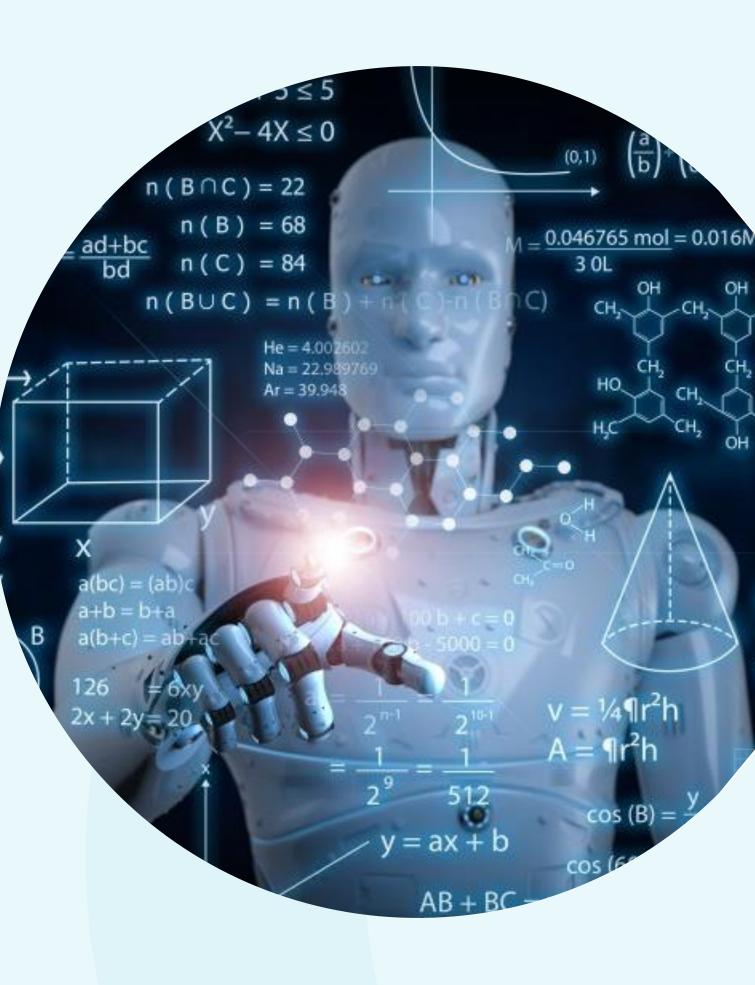  - Individuals
  - Data Breaches
  - Groups

- Discretionary
  - Various routes
  - Development and Coordination Unit
  - Risk Assessment
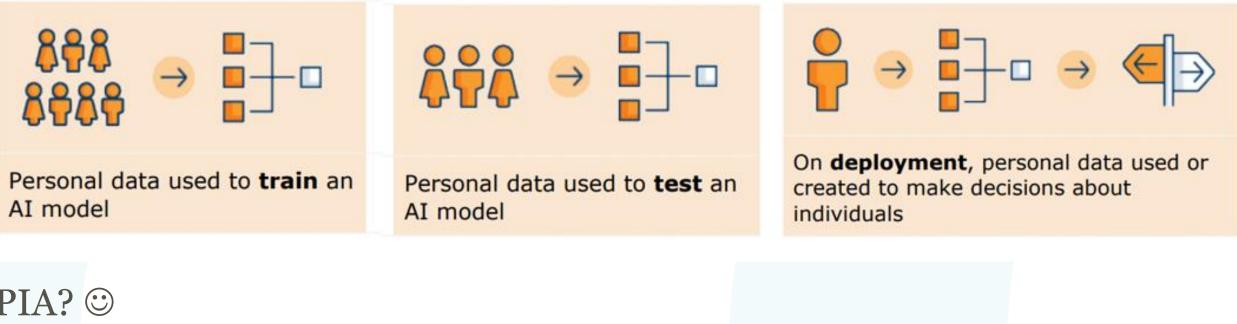  - PACE (Priority, Act Collaborate and Engage

# What does DP Law have to do with AI & Data Science?

ico.

Information Commissioner's Office

# What does DP Law have to do with AI and Data Science?

- UK GDPR and Data Protection Act 2018 regulate *processing* of *personal data*
- Personal data is widely defined
- Where AI doesn't involve use of personal data, falls outside scope of data protection regime

- When is personal data being used?



Personal data used to **train** an AI model

Personal data used to **test** an AI model

On **deployment**, personal data used or created to make decisions about individuals

- Key Questions:

0. Have you done a DPIA? ☺

1. Is personal data being used fairly, lawfully and transparently?

2. Do people understand how their data is being used?

3. How is data being kept secure?

# AI and Data Protection Guidance & Toolkit



Accountability and governance in AI — 1

Fair, lawful and transparent processing — 2

Data minimisation and security — 3
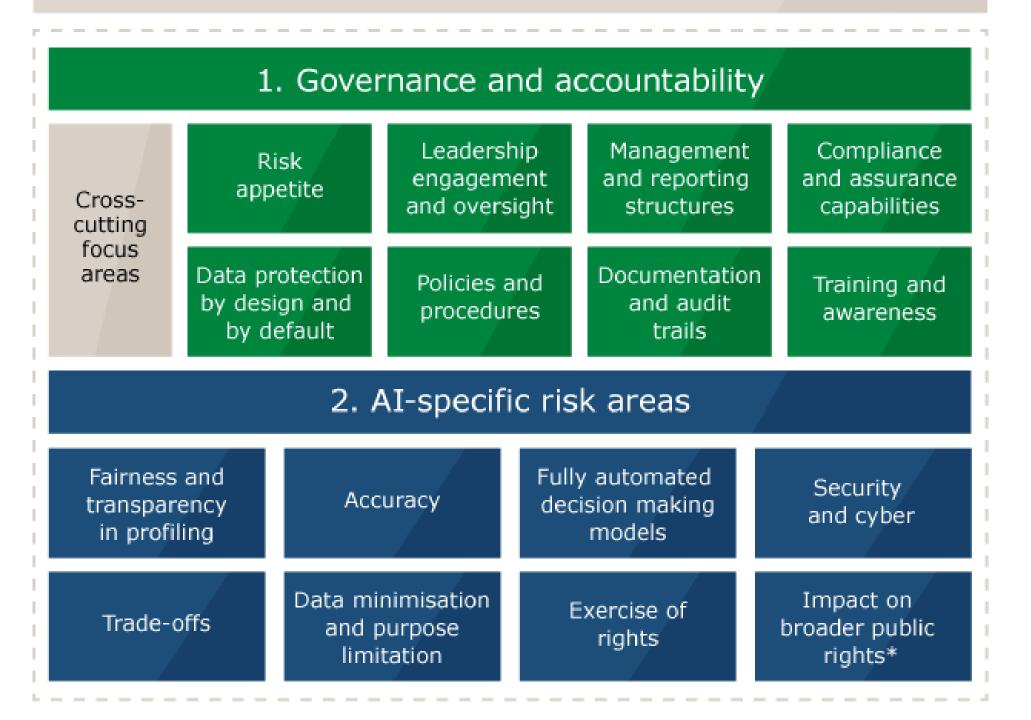
Compliance with individual rights — 4

ico.

https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/guidance-on-ai-and-data-protection/
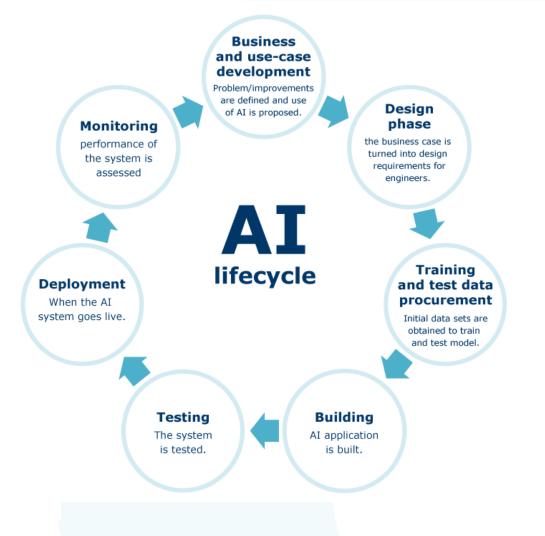
# Auditing Framework for AI and its core components



## Proposed framework

### 1. Governance and accountability

| Cross-cutting focus areas | Risk appetite | Leadership engagement and oversight | Management and reporting structures | Compliance and assurance capabilities |
|---|---|---|---|---|
| | Data protection by design and by default | Policies and procedures | Documentation and audit trails | Training and awareness |

### 2. AI-specific risk areas

| Fairness and transparency in profiling | Accuracy | Fully automated decision making models | Security and cyber |
|---|---|---|---|
| Trade-offs | Data minimisation and purpose limitation | Exercise of rights | Impact on broader public rights* |

*Includes only considerations within scope of an ICO investigation/audit



**AI lifecycle**

**Business and use-case development** — Problem/improvements are defined and use of AI is proposed.

**Design phase** — the business case is turned into design requirements for engineers.

**Training and test data procurement** — Initial data sets are obtained to train and test model.

**Building** — AI application is built.

**Testing** — The system is tested.

**Deployment** — When the AI system goes live.

**Monitoring** — performance of the system is assessed

https://ico.org.uk/about-the-ico/media-centre/ai-auditing-framework/

# Some of our related work



ico.
Information Commissioner's Office

# Guidance / Opinions / Reports / Toolkits (1/2)

- [Guidance on AI and data protection (2020)](#) – this overarching guidance covers what we think is best practice for data protection-compliant AI, as well as how we interpret data protection law as it applies to AI systems that process personal data.

- [Explaining decisions made with AI (2020)](#) – this co-badged guidance by the ICO and The Alan Turing Institute developed as part of [Project ExplAIn (2019)](#) aims to give organisations practical advice to help explain the processes, services and decisions delivered or assisted by AI, to the individuals affected by them.

- [Age Assurance for the Children's Code (2021)](#) - this Opinion is for providers of Information Society Services (ISS) in scope of the code, and providers of age assurance products, services and applications that those ISS may use to conform with the code. Section 4.2 looks at age assurance and AI.

# Guidance / Opinions / Reports / Toolkits (2/2)

- [AI and data protection risk toolkit (2021)](#) – our AI toolkit is designed to provide further practical support to organisations assessing the risks to individual rights and freedoms caused by their own AI systems.

- [Toolkit for organisations considering using data analytics (2020)](#) – this toolkit helps organisations recognise some of the central risks to the rights and freedoms of individuals created by the use of data analytics.

- [Big data, artificial intelligence, machine learning and data protection (2017)](#) – this discussion paper looks at the implications of big data, AI and ML for data protection, and explains the ICO's views on these.

- Of course there are many other relevant opinions, consultation responses and governance sandbox reports which are all [publicly available online](#)
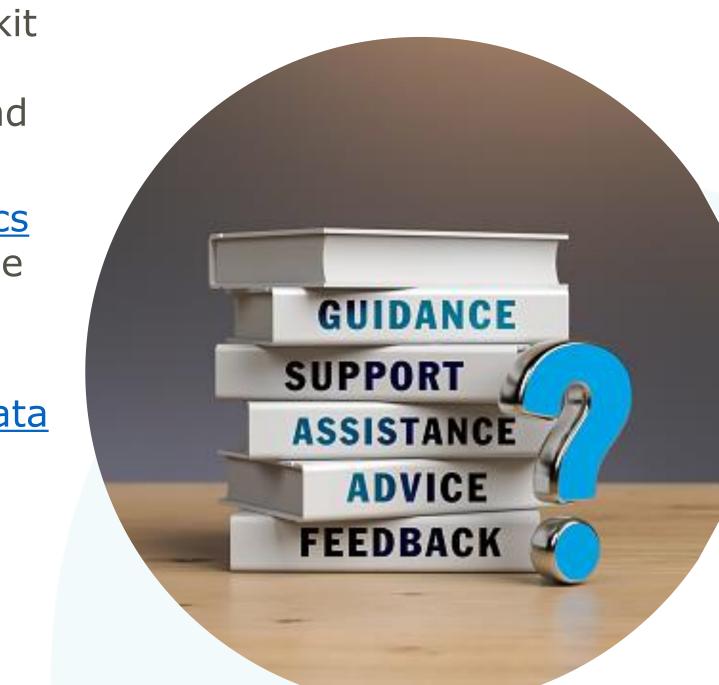
# Current focus/issues being considered

# What are we currently working on? (1/2)

- **Fairness in AI** – This is an update to our AI & Data Protection guidance on how organisations should interpret the fairness principle as it applies to AI, along with good practice in terms of organisational and technical measures

- **AI As A Service (AIaaS)** – This will extend our Cloud Computing Guidance (2021) to provide specific guidance to organisations seeking procure AI-As-A-Service from vendors esp. with regards to assignment of controller and processor roles

- **Algorithmic Content Recommendation Systems** – This is novel research that will seek to clarify how data protection and privacy laws apply to content recommendation systems that may recommend harmful content to children or other vulnerable groups

# What are we currently working on? (1/2)

- **Dark Patterns** – This research seeks to clarify the relationship between dark patterns and data protection law relating specifically to AI systems – specifically through the lens of misuse of personal data and its role has within dark patterns

- **Model Inference Attacks** – This is novel deep research into how to provide technical and governance guidance on how to prevent and mitigate against model inference attacks – can a learned AI/ML model be used to re-identify subjects? Can an ML model be described as sensitive data and hence need data protection and privacy laws applied?



Image from: Unsplash

# ICO Regulatory Sandbox & iAdvice Service (2023)

- Exploring definition of special category biometric data

# Questions

Thank you for listening. Happy to answer any questions online and offline – {technology, ai}@ico.org.uk

@ICOnews