



AMBERHAWK

GDPR IN THE AI AGE

**BCS People, Data and AI Conference;
June 10, 2026 in London**

Dr. C. N. M. Pounder
Amberhawk Training Limited



START WITH TWO FUNDAMENTAL DP ISSUES

1. Is the data protection regime engaged?

- Is the information processed “personal data”?
- Is the organisation processing as a “controller” or “processor”?

NOT PERSONAL DATA (e.g. ANONYMOUS)? NOT A CONTROLLER?

2. If the DP regime is engaged then with respect to personal data:

- Is the processing lawful in general (e.g. has a lawful basis)?
- Is the further processing incompatible with obtaining purpose?

STOPS UNLAWFUL PROCESSING OR INCOMPATIBLE PROCESSING?

If a **controller** processes personal data then it has to meet all the DP obligations (e.g. Data Protection Principles, data subject rights, security, DPIA, data breach, transfer, accountability). **Processor** obligations limited to security, transfer and contractual issues

IN AN AI PILOT, CONSIDER PSEUDONYMISATION TO PROTECT DATA SUBJECTS' IDENTITY



ID DETAILS plus Pseudonymiser No.

Pseudonymiser No. plus ATTRIBUTES

Identification DS(n)	x	↔	x	Attributes of DS(n)
Identification DS(n+1)	y	↔	y	Attributes of DS(n+1)
Identification DS(n+2)	z	↔	z	Attributes of DS(n+2)

ENCRYPT THE SEPARATE “IDENTITY DETAILS” DATABASE AND APPLY HIGH STANDARD SECURITY CONTROLS SURROUNDING ACCESS TO IT

x	Attributes of DS(n)
y	Attributes of DS(n+1)
z	Attributes of DS(n+2)

***This is the
Pilot AI
dataset to
be used***

Data subjects can be re-identified via authorised access/decryption of the encrypted pseudonymised identity (i.e. very auditable!)

LAWFUL PROCESSING? EU AI ACT DEFINES PROHIBITED AI DEVELOPMENT BY LAW



UNLAWFUL PROCESSING OF PERSONAL DATA IN THE EU. Banned high-risk AI Systems: penalties up to €35million or 7% global turnover

- harmful AI-based manipulation, deception or exploitation of the vulnerabilities of individuals
- social scoring
- individual criminal offence risk assessment or prediction
- untargeted scraping of the internet or CCTV material to create or expand facial recognition databases (*e.g. Clearview's scraping?*)
- emotion recognition in workplaces and education institutions
- biometric categorisation to deduce protected characteristics
- real-time remote biometric identification for law enforcement purposes in publicly accessible spaces

ADDED RECENTLY: Nudification applications

LAWFUL PROCESSING? FOR A PILOT AI PROJECT



- Lawful basis for the AI training/testing is likely to be “**legitimate interests**” or “**public task**” (for the public sector).
- “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 ...of the data subject...**”
- **If**, in a pilot AI project, there is **no impact/decision on any data subject** then it is going to be difficult for most data subjects to demonstrate an **overriding** legitimate interest. “**NO impact**” usually protects the data subject’s legitimate interests.

Discuss with your DP specialist to ensure your live AI system has a lawful basis. If confidential or special category of personal data are processed additional considerations apply to the AI Pilot

INCOMPATIBLE PROCESSING? SHOULD NOT BE A PROBLEM IN AN AI PILOT



- The Data (Use and Access) Act 2025 states that the processing of personal data for a **further** purpose is to be treated as processing in a manner compatible with the original purpose when

“the processing is carried out for the purposes of ensuring that processing of personal data complies with Article 5(1) or demonstrating that it does so” .

- As the processing purpose is to test if the Principles are satisfied (e.g. AI Algorithm fair; accuracy; data minimisation), ***this infers that the test could prove that a Principle is not satisfied*** (i.e. breached)
- Unlikely that the AI Pilot will create ICO enforcement problems with respect ***to the ONLY the Principles in A.5(1), especially as, in theory, there is no impact/decision on any data subject.***

6

MUST adopt an appropriate robust approach to other (non-Principle) obligations (e.g. Accountability, data breach, **security**, transfers, rights)



DPIA RISK ASSESSMENT? WHEN TO DO ONE

- DPIA risk assessments **are mandatory** when processing is likely to result in **high risks to “the rights and freedoms of individuals”** (A.35)
- ICO states that when “*processing involving the use of innovative technologies, or the novel application of existing technologies (including AI)....a DPIA is required where this processing is combined with any of the criteria from the European guidelines*” (these criteria and guidelines are found in a document reference “WP248”).
- As there is no “combined” processing AND no impact/decision on most data subjects, there is not a **high risk** to most data subjects so there is **no need to do a DPIA** for the pilot/testing phase
- If ICO changes his mind over DPIA for AI Training, the lack of any impact/decision on any data subject makes the processing low risk
BUT DPIA **is needed** **BEFORE** AI is incorporated into active systems



ACTIVE AI (HIGH RISK NEEDS A DPIA)

UK's ICO (**and** WP248 classifications) mandate a DPIA when using innovative technology such as AI to deny data subjects a service, contract or right etc. Remember focusing “*resources on people in need*” is exclusionary for people “*not quite in the same need*”.

A DPIA is needed if controller decides access to services/jobs etc:

- using profiling or special category of personal data (e.g. health, political, ethnicity, sexual orientation) in decision taking
- profiling individuals on a large scale;
- matching or combining personal datasets from different sources;
- profiling children or target marketing or online services at them
- processing personal data that might endanger the individual's physical health or safety in the event of a security breach

ESSENTIAL to discuss DPIAs with your DP specialist

HIGH RISK “DPIA” CATEGORIES IN THE EU AI ACT



Biometrics (Facial recognition/biometric data processing); Critical Infrastructure (Essential services in energy, transportation, water); **Education and Vocational Training (Educational assessments and training programs); Employment Management (Hiring, performance evaluation, and employee management); Access to Essential Services (Access to essential private or public services and benefits);** Law Enforcement (Policing, surveillance, and crime prediction); Migration, Asylum, and Border Control (Immigration processes and border security). [The ones in **BLUE** and **RED** might be already active!]

Mandatory safeguards include: technical documentation available, EU database registration, **risk assessments (e.g. DPIA)**, human oversight protocols, and ongoing monitoring for serious incidents. Organisations must demonstrate that previously completed human assessments are less effective than AI-assisted decision-making.

MUST MAKE AN AI PILOT TRANSPARENT (A.13;A.14)



Change the Privacy Notice to include the statement on the lines of:

- *“It is in our legitimate interests to plan to use your personal data to improve and develop our services to you using AI techniques. **Whilst testing the system to identify the best and safest AI techniques to use, we protect your legitimate interests by not having any impact on the services we offer to any customer or any potential customer”.***

Add the missing A.13&A.14 requirements (e.g. lawful basis, right to object, recipients, transfers, retention) to cover the AI Pilot. ***Liaise with your DP specialist*** (as required)

Offer an opt-out? ***Answer = NO*** because ***NO IMPACT*** means the legitimate interests of the data subject have been taken into account

Privacy Notice ALSO needs changing if the AI system goes live.

AN AI PILOT CAN TRIAL AUTOMATED DECISIONS



- The right not to be subject to an automated decision/profiling has been changed to permit decisions/profiling in most circumstances.
- An automated decision: (1) relies **solely** on the processing of personal data; (2) has significant impact on the data subject **and**, (3) has “*no meaningful human involvement*” in the decision.
- **If the AI pilot**, has **no automated decision** or **profiling** which has a *significant decision* or *legal effect* on a data subject, then the AI pilot project is **not** subject to this right.
- However, the UK_GDPR defines a limited subset of conditions when a controller **cannot** make automated decisions/profile (e.g. when processing special category of personal data such as health).
- **Essential you discuss with your DP specialist** if the AI pilot is using special category of personal data (e.g. health records) to ensure your live AI system is not prohibited.

TRANSPARENCY “MUSTS” BEFORE AI GOES LIVE



Implement statutory safeguards for automated decision taking:

- Provide **the** data subject with meaningful information **prior** to any automated decision taken, or profiling of, the data subject
- After a decision has been taken, enable the data subject to:
 - make representations about their decision
 - obtain human intervention re a decision
 - contest a decision
 - understand why the decision was taken
- Follow up on a representative sample of decisions (e.g. chase down false positives or false negatives)
- Check there is no bias in, or false assumptions made, in any mathematical or statistical technique used

12

Liaise with your DP specialist about changes to the Privacy Notice



SUMMARY OF DP ISSUES ON A LIVE AI SYSTEM

- Carry out a DPIA if profiling or making automated decisions are on the ICO's **high risk** radar; EU AI Act lists **high risk** use of AI.
- Identify lawful basis; check for incompatibility of **further** processing
- Ensure that the use of personal data is lawful in general (e.g. does not breach: a confidence; a prohibition; copyright; a contract)
- Ensure transparency, fairness, anti-bias and safeguards (slide 12) are implemented in addition to any Privacy Notice change
- Dealing with the Principles (e.g. accuracy; retention; minimisation)
- Dealing with rights of data subjects (objection, correction, access)
- Security requirements (e.g. data breach) and transfer obligations
- Manage the expected security/transfer standards with Processors
- Accountability requirements and management reporting in general

MUST liaise with your DP specialist for all of the above.

KEEP ABREAST OF CHANGES TO ICO GUIDANCE AND DSIT POLICY ON AI



“Old” AI Guidance to be re-issued this Summer in final form

What's new?	2
About this guidance	5
What are the accountability and governance implications of AI?	12
How do we ensure transparency in AI?	28
How do we ensure lawfulness in AI?	29
What do we need to know about accuracy and statistical accuracy?	38
How do we ensure fairness in AI?	44
What about fairness, bias and discrimination?	53
What is the impact of Article 22 of the UK GDPR on fairness?	69
How should we assess security and data minimisation in AI?	72
How do we ensure individual rights in our AI systems?	89
Annex A: Fairness in the AI lifecycle	105
AI and data protection risk toolkit	135
Glossary	136

The Data (Use and Access) Act 2025 requires changes to sections dealing with transparency, lawfulness, fairness and bias, discrimination, A.22, data minimisation, rights and governance

LIMITED AND MINIMAL/NO RISK AI SYSTEMS IN THE EU AI ACT



Limited Risk. There is a focus on transparency when using generative AI systems and large language models. **Must** inform users that they're interacting with AI.

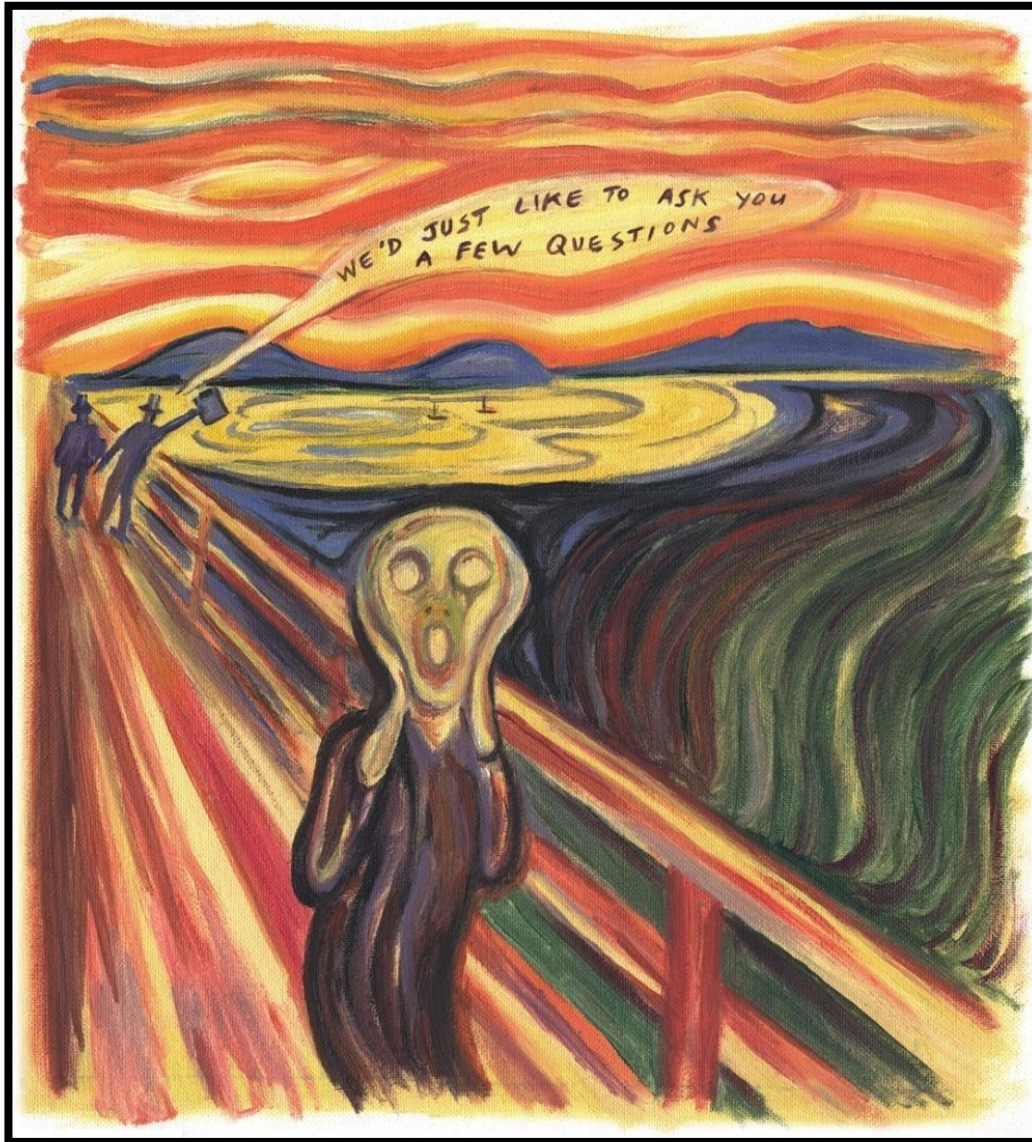
However, general-purpose AI models deployed on technology exceeding performance of 10^{25} FLOPs face extra obligations, including model evaluation and incident reporting. Additionally focus on user awareness of AI use and responsible implementation/deployment.

Minimal or No Risk AI Systems AI applications. Covers all AI applications ***not in the prohibited, high risk or limited risk categories.*** (e.g. AI-enabled video games, spam filters, recommendation systems). Developers expected to adopt voluntary codes of conduct and ethical AI principles. **No** mandatory obligations under the EU AI Act.

GDPR in the AI Age



Q
U
E
S
T
I
O
N
S



More on the
GDPR in all
our DP
officer
courses
and on
HAWKTALK
(wholly balanced blog)

©Chris Slane



AMBERHAWK

GDPR in the AI Age

June 2026

©Amberhawk Training Limited