Submitted by: [redacted]

Date: 15 June 2026

These submissions are being made in a personal academic capacity. My research sits at the intersection of artificial intelligence, data law, and the governance of automated systems, especially in public administration, so I am drawn to how legal obligations translate (or fail to translate) into technical implementations. My doctoral work examines risks and opportunities of European Data Spaces, a concept devised for ease of sectoral data flow across institutions without breaching the law. [redacted] GEMS project (Games as Multi-layered Security Threat, Horizon Europe), which examines how digital platforms mediate harm to vulnerable communities.

I write from this position because the questions the Issues Paper raises, about what counts as a 'decision', who counts as 'vulnerable', and what transparency actually requires, are not merely legal questions I believe. They are questions about how technical systems encode social assumptions. My response draws on comparative analysis of the EU GDPR (Article 22, etc.), the Council of Europe's Convention 108+, and my own published work on machine learning systems and privacy rights.

## Question 1

Rankings (1–5):

- Degree of reliance on the ADM system output: 5
- Nature of the output (advisory vs determinative): 4
- Integration of ADM into decision-making workflow: 2
- Ability and likelihood of human override: 2
- Transparency and explainability of outputs: 5 — affects quality of human review, not the threshold

Free text:

The primary factor in whether a computer program is substantially and directly related to a decision are how much we are relying on that output, and in the case of grievances

etc., whether we can explain that output. These are ranked highest because they are the factors most resistant to manipulation by entities seeking to avoid the obligation.

By contrast, integration into decision-making workflow and the ability and likelihood of human override are ranked low. These are not irrelevant, mind you, these are just open to more interpretation and often manipulation. An entity can formally document human oversight, build override capacity into a workflow, and integrate an ADM system in ways that appear procedurally compliant, while the substantive weight of the ADM output on the final decision would remain completely unchanged. I will venture to say these are self-reported, and not meaningful in the same way dependence on AI or explainability of used AI is. What is integration? It could be anything from a writing assistant to a man in the high castle. What is human override? How much override is the human doing? Are they just looking at it? Are they observers? Do they have agency when the decision tree becomes too complex?

The EU Guidelines on Article 22 GDPR (Article 29 Working Party, 2018) recognised this by noting that 'rubber-stamping' of automated outputs does not satisfy the meaningful human review requirement. A system that produces score or risk rating or recommendation that is accepted as a part of a routine is directly related to the decision, regardless of what the privacy policy says about human involvement.

## Question 2

Answer: Yes

Reason:

GPTea's outputs are dictating individual eligibility decisions. I mean, the human review is structurally constrained by volume pressure, high stakes, and the AI summary substituting for independent case review. Formal oversight is not meaningful oversight. I mean, with so many elders, do we have enough workers to review the nitty gritties of these summaries? Do we know yet why the output is the way it is? How GPTea was even trained or on what data?

## Question 3

Rankings (1–5):

- Vulnerable persons: 5
- Sensitive information: 5
- Financial outcomes: 3
- Intrusive practices: 3

Free text:

Financial outcomes and intrusive practices are ranked at 3 because their significance is depending on other things, like a financial impact can be severe if and when the subject has limited financial means, or an intrusive practice matters most when subject is already vulnerable or the information is already considered sensitive. Without vulnerability or sensitivity as multipliers, these factors don't independently signal that rights or interests are significantly affected. Also another thing not listed is how reversible is the damage. If it's irreversible, severity becomes more extreme.

## Question 4

The following classes (at least) should be explicitly recognised as vulnerable: children, elderly people, people with limited financial means, LGBTQ+ people, racially and ethnically marginalised communities that are citizens but are not treated as such, and persons with disability. Vulnerability can multiply when you belong to more than one of these categories, a 70 year-old black lesbian woman whose family has been there for six generations in a country like Australia faces a risk profile more convoluted and discriminatory than any single category can even suggest. Guidance that treats vulnerability as a yes-no binary will fail people most affected by systems. Automated decisions systems trained on biased data may misclassify gender, identity, or other features, and then can generate compound errors in healthcare, immigration, social services etc. contexts where the consequences are most difficult to reverse. Vulnerability is not always even self-evident or self-reported, this reinforces the case for proactive disclosure and a look into who are vulnerable, keeping track actively, rather than disclosure that comes after individual request.

## Question 5

Rankings (1–5):

- Access to essential banking and credit services: 5
- Physical assistance/ support: 5
- Financial assistance: 3
- Access to healthcare services: 5
- Access to essential utilities: 5
- Access to telecommunications: 3
- Access to educational services: 5
- 'In home' services: 3

Free text:

Employment opportunities should be added as a significant service or support, even if it's private institutions hiring people. Algorithmic exclusion from job advertising has effects many many people (ATS systems are known for excluding women, people of color, etc. and yet we use them). OAIC could have a deeper look at it.

## Question 6

Article 29 Working Party / EDPB Guidelines on Automated Individual Decision-Making and Profiling (2018) contain the most developed international analysis of meaningful human involvement and similarly significant effects. Like they have this position that profiling-based advertising limiting employment opportunities is within its scope, which is directly applicable to Question 8. Very important for OAIC.

And then, Council of Europe Convention 108+ (2018) is a better framework for Australian legislative design than GDPR, because it is more flexible and less attuned to European realities. It has in its Article 9 safeguards against automated decisions that significantly affect individuals, including the right to human intervention and explanation. Explanation to me is very very important in all of this. If I am to be tried for a crime, at least I should know what crime it was that I am being accused of (AI is very Kafkaesque in this regard).

And then there is this EU AI Act. Its article 86 establishes an emerging international standard for the right to explanation in high-stakes automated decision contexts. Learning from GDPR and adequacy decision fiascos, it's good not too have too much of divergence between Australia and EU.

## Question 7

Does the price inflation significantly affect Marco's interests? Yes.

On the threshold question:

Yes, any differential pricing of anything significantly affects our interests, this threshold question is just a distraction. Pricing based on personal data to produce different outcomes for different individuals is a decision that affects our rights and interests. This is the thing about such decision making, why would a seller need to know my credit score? It's bad enough that hospitals discriminate also based on this. The OAIC should treat differential pricing derived from personal data as violating people's rights rather than asking how much differential is too much differential.

Factor rankings (1–5):

Significance of the product or service being purchased: 1

Dollar amount of differential pricing: 1

## Question 8

Should it be considered a 'decision' that Rafqa did not receive the Manscon job ad? Yes.

Reasons:

Opaque window's non-delivery of the advertisement to Rafqa is a decision in the most relevant sense. The fact that it happened to happen by omission rather than affirmative refusal does not change much. My work with Europol and Trinity College Dublin on digital exclusion of vulnerable communities confirms something of interest here, to quote, that "algorithmic targeting which structures access to communities" must be legally inspected. Not showing an ad to women is tantamount to rejecting all women.

## Question 10

The OAIC's proposed disclosure principles (plain language, structured, tailored, logical, contestable) are sound. I would add the following:

- Proactive notification at the point of decision, for transparency
- Disclosure of known differential error rates across demographic groups, like a system 95% accurate overall may be significantly less accurate for the communities it most affects (see the works of Timnit Gebru or Abeba Birhane for example)
- A named, specific contact pathway for grievance etc., not a general privacy policy address. Like a person who can be contacted when things go south.