

Data Controller Survey – Summary of qualitative findings

Use of technologies by data controllers in the UK

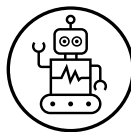
20 qualitative interviews with organisations that took part in Year 2 of the Data Controller Study survey were conducted in February and March 2025. The interviews were focused on the use of technological processes to process personal data. This included:



Anonymisation
pseudonymisation



Biometric or facial
recognition



Artificial
Intelligence (AI)



Automated Decision
Making (ADM)

Uptake and familiarity



Familiarity and uptake of the technologies studied were low, particularly AI and ADM.

Looking to the future



Future uptake varied:

- Most organisations did not expect an increase in the use of biometrics, anonymisation or pseudonymisation.
- Organisations had opposing views on the future adoption of AI and ADM.

"We just don't know enough about [AI]"
– Medical practice

"We'd have to change radically to for us to consider [AI]." - Local town council

"[The rise of AI] is inevitable, it's happening already"
– Film and editing firm

Costs and benefits of implementation

- + Improves security and limits harms for unauthorised access:** organisations reported feeling more secure with technologies such as anonymisation, pseudonymisation and biometric recognition technology in place.
- + Enables data sharing:** anonymisation and pseudonymisation allow organisations to share data with other organisations and the public.
- + Increases confidence to share data:** anonymisation and pseudonymisation can increase public trust and citizen engagement by safeguarding personal data
- + Drives efficiency:** technology like AI and ADM can free-up valuable employee time for tasks such as note-taking or research.
- Early in the adoption cycle:** the full potential of technologies like AI and ADM are yet to be realised. Organisations are concerned over technological immaturity.
- Concerns around data sensitivity:** Organisations raise that some individuals are worried about their data (particularly sensitive data like biometrics) being processed in unfamiliar ways.
- Ensuring suitable staff training and awareness** is required to promote secure data management, particularly where sensitive data is processed. This has been particularly challenging with readily available AI software.
- Unsuitable for sensitive decisions:** several organisations reported that the decisions they make are too complicated and nuanced to be left to ADM or AI.

"If [citizens] know that [their responses] are not going to be shared more widely [...], it might encourage more people to engage with us." – Town council on the use of anonymisation

"It's quite difficult for a local authority that is so accountable for its decision making to use ADM... there will always be unique circumstances that have to be taken into account."
– Government body on the use of ADM