Ada Lovelace Institute

Transparency mechanisms explainer
For Government, local government, policymakers and researchers

Transparency mechanisms for UK public-sector algorithmic decision-making systems

A review of existing UK mechanisms for transparency, and their contribution to making public information relating to the implementation of algorithmic decision-making systems (ADMs).

Introduction

We currently have a fragmented landscape of mechanisms for transparency that, taken individually or combined in the limited ways currently possible, leave us far from ensuring that we are capable of scrutinising and evaluating the functions, or effects on communities and individuals, of ADM systems in use or under consideration in central or local government.

In order to obtain meaningful transparency there are some key questions that need to be answered, for example:

- What are the data sources of a system?
- Who is operating it?
- What are the conditions around repurposing or using it in other contexts?
- Why is the system being developed?
- What were the alternatives and how was a specific ADM system selected?
- What is the logic of the system?
- Who built it and how much did it cost?
- Were private actors involved?
- Are there specific impacted groups, and how are they impacted?

This information is nominally available in transparency documents that are produced by local and central government and public-sector officials. In practice these documents and information are seldom released into the public domain, and if they are released, are not organised or made available in ways that make it easy to consult.

These limitations are compounded by the reality that some existing transparency protocols are not currently mandatory, or not mandatory for ADM systems; some are mandatory but not effectively enforced; and those that are mandatory could be better promoted through best-practice guidelines that offer practical support to over-resourced public authorities.

To create coherence out of this landscape, and systematically strengthen transparency practices across government, we have focused on currently underused informational assets that, taken together (if not individually), can enable us to make meaningful extractions and inferences about the way ADM systems are used across government.

Contents

1. Assessments and evaluations
2. Procurement and spending documents
3. Open source/open data standards
4. Freedom of information and subject access requests
5. Standardised disclosure of data used or produced in the deployment of ADM systems

The purpose of this review is to survey these mechanisms and their effectiveness. While we acknowledge the relevance and importance of transparency mechanisms that are specific to different domains of public life in which ADM systems may be implemented, this review does not consider them explicitly.

However it is worth noting that organisations such as the Joint Council for the Welfare of Migrants, Which?, Citizens Advice, Child Poverty Action Group, among others, have acted on multiple occasions, and with a variety of research and policy contributions, in order to foster algorithmic transparency and accountability in their particular areas of expertise. These organisations can be considered key actors in the transparency policy domain and their expertise should be mobilised as important to the debate, and also in order to take part of the burden of ensuring transparency away from affected subjects and support them through the process of achieving accountability and redress.

1. Assessments and evaluations

Impact assessments (IAs):

Impact assessments (IAs) aim to anticipate the ramifications of a specific public policy intervention with a view to identifying any risks or consequences that may need to be mitigated. They are used across different sectors in the form of environmental IA, human rights IA and equalities IA, as post-hoc and ex-ante mechanisms.

As clarified in our report, *Examining the Black Box*, impact assessments that focus specifically on algorithms can refer to processes conducted before, during or after deployment, as risk assessments or impact evaluations.

While these mechanisms are still being tested, they are far from being an established practice, let alone a regulated requirement in most jurisdictions for instance Canada has been trialling algorithmic IAs, based on a mode that establishes degrees of risk implicated in the implementation of the algorithmic system and mitigation processes required through a questionnaire.

For ADM systems, the type of assessment currently in use is the data protection impact assessment (DPIA), which is a process intended to identify and minimise risks from the perspective of data protection.

Given the complexity of ADM systems, the effort to identify responsible bodies for the exercise of scrutiny (and consequently the implementation of relevant IAs) has sparked debate,[1] as well as a number of calls for new regulatory bodies, expert groups and commissions.[2]

Data protection impact assessments (DPIAs):

Arguably, DPIAs constitute the most productive tool for illuminating the function and social dimensions of ADM systems, as their remit covers a wide range of information, including data fields and sources, the system's function within broader administrative processes, the responsible officials, and the effects and legal basis for data processing.

The organisation controlling the data processing is responsible for producing the relevant DPIA, even if the production of the document is outsourced to a data processor. The data controller must seek advice from its data protection officer, as recommended by guidance from the Information Commissioner's Office (ICO).

Some limitations of DPIAs, as currently used, are:

- they are not typically accessible in the public domain
- the guidance on the circumstances under which they are mandatory is not conclusive
- their format displays huge amounts of information that is not intuitively translatable into the effects an ADM system may have on people and communities.

In terms of their legal status and functionality, according to the GDPR (Article 35), DPIAs are supposed to consider the 'risks to the rights and freedoms of natural persons' and, as highlighted by the ICO guidance regarding GDPR Recital 75, risk is linked to potential harm to individuals, which includes 'processing [that] may give rise to discrimination' and 'significant economic or social disadvantage'.

---

1 In the UK, the Committee on Standards in Public Life has recently weighted against the establishment of a new regulatory body and recommended that: 'The Equality and Human Rights Commission should develop guidance in partnership with both the Alan Turing Institute and the CDEI on how public bodies should best comply with the Equality Act 2010'. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/868284/Web_Version_AI_and_Public_Standards.PDF. This type of guidance through partnership is also exemplified by the guidelines for carrying out DPIAs on surveillance camera systems, jointly published guidelines by the ICO and the Surveillance Camera Commissioner. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/881538/SCC___ICO_DPIA_guidance_V3_FINAL_PDF.pdf. In Europe, a similar effort is exemplified by the Digital Clearinghouse, which aims to create 'closer cooperation and coherence between different regulators'. Available at: https://edps.europa.eu/data-protection/our-work/subjects/big-data-digital-clearinghouse_en. The recently established Regulatory Horizons Council in the UK has comparable ambitions. Available at: https://www.gov.uk/government/groups/regulatory-horizons-council-rhc.

2 See for example Lord Justice Sales's proposal of an algorithm commission, available at: https://www.supremecourt.uk/docs/speech-191112.pdf; Access Now's EU White Paper Consultation Submission, available at: https://www.accessnow.org/cms/assets/uploads/2020/06/EU-white-paper-consultation_Access_Now_June2020.pdf or Doteveryone's work on Regulating for Responsible Technology, available at : https://doteveryone.org.uk/wp-content/uploads/2018/10/Doteveryone-Regulating-for-Responsible-Tech-Report.pdf

Following this guidance, it has been argued that the scope of DPIAs must extend beyond data protection and into human rights. This would make them more effective and expand their role beyond the enforcement of data protection compliance, a concern raised by stakeholders in the context of the project ExplAIn conducted by the ICO and the Alan Turing Institute.

DPIAs are mandatory when the data processing under consideration is deemed to 'result in high risk'. However, this is not clearly delineated: the GDPR does not offer a definition of high risk and, while the ICO has published a list of processes that are likely to result in high risk, this is not exhaustive. The guidance also suggests the possibility of not carrying out a DPIA in cases that are appropriately justified and documented.

The ICO states, 'the question [to be asked] is a more high-level screening test: are there features which point to the potential for high risk? You are screening for any red flags which indicate that you need to do a DPIA to look at the risk (including the likelihood and severity of potential harm) in more detail.'

The fact that the guidance on DPIAs is open to interpretation or negotiation means that it might not be compelling enough for organisations, particularly local authorities with limited resources, to invest appropriate time and energy into the assessment of the systems they are operating.

There is also a more general consideration that, in the absence of guidance defining the functions of ADM systems, local authorities may see them as merely digitising existing administrative functions, contributing to the perception that DPIAs are not necessary.

Equality impact assessments:

Another regulatory tool, effective in measuring impact and associated with IAs, is the equality duty created by the Equality Act 2010, which stipulates that public bodies should have 'due regard' to the need to 'eliminate unlawful discrimination, harassment and victimisation, advance equality of opportunity between different groups, [and] foster good relations between groups'.

However, in the context of ADMs in use in government, the effects of the equality duty risk being limited. While public offices are required to assess how their activities impact on equality, how they do so – meaning which process they follow for the assessment – is under-determined, and individual authorities are able to choose a different model.

The Equality and Human Rights Commission states in the Specific Duties FAQs that 'having due regard to the aims of the general equality duty is about informed decision-making, not about carrying out particular processes or producing particular documents.' Ultimately, this means that, while due regard is stipulated by the law, no specific mechanism for assessment is enforced.

The Equality Act falls short of protecting people from discrimination that is conducted on the basis of 'categories' that are not protected in the act (such as class).[3] Given the wide reliance on consumer segmentation data (often provided by credit reference agencies, which can be highly exposing of socio-economic status)[4] in the delivery of public services at the local level, there may be a need for a reconsideration and expansion of protected characteristics, in view of recent consumer profiling practices. The composition of current categories means that, even if an authority decided to conduct an equality IA and make it public, it would be insufficient in assessing the various ethically challenging forms of discrimination that ADM systems may result in.

In Scotland, the Scottish Human Rights Commission and the Equality and Human Rights Commission have been developing good practice guides and piloting programmes for joint equalities and human rights IAs. This raises interesting questions about whether a similar project can be undertaken in relation to ADM systems, and, more significantly, about whether and how public bodies outside the realm of technology and information should be engaged to exert more influence on the assessment of ADM systems.

3 A key source of information to help with understanding equalities in the UK today is the Office for National Statistics equalities data audit. The report audits data sources and publications on 71 outcomes for the nine protected characteristics covered in the Equality Act 2010, to inform policy. It is informed by the EHRC's 'Measurement framework for equality and human rights' and the OHCHR 'A human rights-based approach to data' report.

4 See for example, Durham Constabulary's use of Experian's Mosaic dataset. Available at: https://www.bbc.co.uk/news/technology-43428266

Existing calls for mandatory impact assessments:

The AI Now Institute has made a call for algorithmic impact assessments, which entails public consultation.

The Alan Turing Institute has proposed stakeholder impact assessments. As stated in their

guide for the responsible design and implementation of AI in the public sector: 'You and your project team should come together to evaluate the social impact and sustainability of your AI project through a Stakeholder Impact Assessment (SIA), whether the AI project is being used to deliver a public service or in a back-office administrative capacity.' The guidelines go on to specify that '[w]hen we refer to "stakeholders" we are referring primarily to affected individual persons, but the term may also extend to groups and organisations in the sense that individual members of these collectives may also be impacted as such by the design and deployment of AI systems. Due consideration to stakeholders should be given at both these levels.'

Access Now, in its submission to the Consultation on the 'White Paper on Artificial Intelligence

– a European approach to excellence and trust' has called for a Mandatory HRIA & Disclosure scheme: 'As opposed to a binary risk assessment approach, Access Now argues that, for all applications in all domains, the burden of proof should be on the entity wanting to develop or deploy the AI system to demonstrate that it does not violate human rights via a human rights impact assessment (HRIA) and a mandatory disclosure scheme.'

EDRi, in its 'Recommendation for a Fundamental Rights-based AI Regulation', has

recommended that '[a]ll systems meeting the legal criteria [...] complete mandatory human rights impact assessments throughout the design, development, and ongoing development. Following the recommendation of the Council of Europe Committee of Ministers on the human rights impacts of algorithmic systems, this assessment should include an evaluation of the collective, societal, institutional and governance implications the system poses, and outlining adequate steps to mitigate this. Such impact assessments must be made publicly available. To implement this recommendation, the Commission could consider a mandatory disclosure or notification system.'

Panoptykon, in its submission to the consultation on the 'White Paper on Artificial Intelligence – a European approach to excellence and trust', has written 'We recommend a HRIA system for AI applications that is modelled on the GDPR provisions on data protection impact assessments but with important corrections based on two years of experience with the DPIA. GDPR model should be improved by: (i) introducing a mandatory disclosure scheme, (ii) increasing the role of external reviewers, and (iii) increasing engagement from affected communities and civil society.'

The Committee on Standards in Public Life, in their recent report on AI and Public Life, has recommended that 'Government [...] consider how an AI impact assessment requirement could be integrated into existing processes to evaluate the potential effects of AI on public standards. Such assessments should be mandatory and should be published.'

Pilot evaluations:

Another category of evaluation that can be included alongside IAs are reports resulting from pilot schemes and trials. Pilots are an important mechanism for testing policy interventions and the use of new technologies (as demonstrated by the recent roll out of facial recognition technologies in London and other regions of the UK).

While reports resulting from pilots may eventually be placed in the public domain, this often does not occur within a timeframe that permits action prior to the roll out of technologies.

This points towards the necessity of mandating not only a transparency mechanism, but also a schedule of documentation that should be produced and made public, as well as the governance mechanisms that enable its democratic scrutiny, prior to extensive roll out.

Takeaway 1: Clarity over the duty to produce impact assessments and a wider framing of data protection

Impact assessments risk having limited effect due to their uncertain regulatory status. If the impact to be established relates to the welfare of communities and the wellbeing of individuals within them, then data protection frameworks and assessments, as currently practised, constitute too narrow a framework. Establishing a clear list of ADM systems for which an impact assessment is necessary, and adopting an approach that goes beyond compliance with data protection regulation and includes human rights approaches, will help to mitigate these risks.

2. Procurement and spending documents

Spending data:

Information about ADM systems in use can be obtained by analysing transparency data on public spending. While spending data does not exclusively deal with ADM systems, greater standardisation and transparency in this area would constitute a strong guarantee of what is listed in an ADM register as well as promoting good data practice across Government. The limitation to this use is that records for public spending are often incomplete and inconsistently labelled.

In a report published by the Bureau for Investigative Journalism (TBIJ), Government procurement practices were analysed with a special focus on the Digital Marketplace run by the Crown Commercial Service. The report highlighted transparency issues specifically regarding the G-Cloud Framework – one of the primary avenues through which digital public sector services are sold. The Government-released datasets for purchases made on G-Cloud were published in aggregate form, which meant that the transactions between Government buyers and private suppliers could not be linked to the services offered by these companies.

Similar but more complex issues are also evident in contracting. It is worth noting that organisations such as the Open Contracting Partnership advocate for the adoption of an open contracting data standard. This practice could be extended to spending data released by Government at large (including by local authorities, e.g. spending over £500 or procurement card transactions) where datasets display inconsistencies, especially in the labelling of purchases made from companies supplying ADM system solutions.

Procurement documents / audit trails:

Procurement documents can offer a view into the decision making behind the use of ADM systems, by revealing the deliberative processes driving their purchase. These documents can shed light on the relations between Government departments and, in doing so, provide useful context for solutions that are developed in-house or through public-private partnerships. Procurement transparency is intended to be a vehicle for ensuring fair competition and is relevant not only to the public, researchers and regulators, but also to businesses.

Audit trails, as discussed in the TBIJ report cited above, are required for compliance with the Public Contracts Regulations (2015) and are supposed to be a record of the procurement process, documenting communication with suppliers, internal deliberations, and in some cases, even the search terms used when looking for services. These form a significant part of the narrative of how and why public sector procurements are made but are also an important record of spending in this area.

While it is mandatory to document the procurement process, record keeping in this area appears to be poor and inconsistent at all levels of Government. The Cabinet Office operates a Public Procurement Review Service, primarily with the function of resolving procurement disputes, however the scope of the service extends also to performing spot checks on procurement documents.

(Local) audit reports:

Given the strong tendency in Government to cite economic use of data analytic systems through reference to savings (particularly in the context of austerity), a measure of whether the use of ADM systems is justified is how they are performing against economic indicators.

Local authorities have audit committees tasked with monitoring strategy and managing risk, primarily by carrying out financially focused audits. As noted by the Chartered Institute of Public Finance and Accountancy: 'There is no statutory obligation for a local authority to establish an audit committee.' Nevertheless, establishing audit committees is a widely recognised practice in the public and private sectors. Where they are implemented, committees can exercise oversight over major projects, including decisions on the procurement of technology.

The varied implementation of local audit processes is due to the abolition of the Audit Commission, 'an independent public corporation [operating] between 1 April 1983 and 31 March 2015', which has devolved this function to local authorities.

While local audit committees are not a mechanism designed to assess the procurement of technology specifically, it may be useful to consider how they can be supported to incorporate a technology code of practice into their evaluations of purchasing decisions. In circumstances where a transparency mechanism is recommended, local audit committees could contribute to an ecology of governance bodies that oversee the mechanism and foster scrutiny.

Takeaway 2: Greater transparency in procurement procedures

The transparency documents produced in relation to procurement processes, such as audit trails, spending data and audit reports, can offer significant insights into how and why certain technological solutions are adopted. The poor record keeping of procurement processes constitutes a clear barrier to their use for the purpose of transparency. The mandatory production of audit trails should be adequately enforced and documents that relate to the procurement of technology should be made publicly available in accessible formats.

3. Open source/open data standards

Publishing the source code of an ADM system is possible under specific circumstances and is an increasingly common practice where there is an interest in securing public trust (see, for instance, the case of the NHS COVID-19 contact tracing app). While there is no centralised domain where source code is published, GitHub (an open source development platform) has assumed this function, and is used by some parts of government (see for example the Government Digital Service page on GitHub).

The publishing of source code is an important transparency mechanism. As the purpose of this review is to offer a clarification of the practices that look beyond the technical specificities of ADMs to generate a holistic and cross-cutting view, our focus on open standards is mostly concentrated on how they can supplement the other mechanisms listed here.

In this regard, it can be noted that through the UK Government's digital transformation agenda, there has been a move towards the use/development of open standards and open source (OS) software. Recent guidance by the Government Digital Service (GDS) encourages OS and makes its consideration a condition of meeting point three of the Technology Code of Practice, which sets criteria to help Government design, build and buy technology and is used as the agreed standard in the spends control process.[5]

The spends control process requires the GDS to approve of Government-led projects, classified as 'digital' or 'technology' services. It is stated in the guidance that one of the factors determining how the GDS will decide which services need approval is whether the department making the application is a central government department. It is currently unclear how these principles extend to local authorities.

5 'The Technology Code of Practice is a set of criteria to help government design, build and buy technology. It's used as a cross-government agreed standard in the spend controls process.' Available at: https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-of-practice

However, the ambition of the Local Digital Declaration – a coalition of local authorities and sector-specific organisations, initiated by the UK Ministry for Housing, Communities and Local Government and GDS – to develop an open culture and procure technology according to the technology code of practice may point to ways for this initiative to be taken forward at the local level.

On a more fundamental level, when datasets are published for transparency, they should use an open standard so that anyone can fuurther analyse and inspect their use.

Where this is not implemented, transparency stands to 'intentionally occlude', which in this context can refer to instances where organisations make information seemingly visible, but opaque in practice. For example, the new Digital Marketplace spending website (which contains spending information on the past two years, discussed above in relation to procurement) is hosted on a Microsoft Power BI platform that does not offer a simple option for .csv downloads of the data (which is available for previous years' datasets, like most datasets held under the Open Government license).

There are clear guidelines set out by the GDS Service Standard[6] or in the Local Government Transparency Code on the use of open formats when making data available. These guidelines uniformly recommend non-proprietary formats (such as .csv).

Takeaway 3: Concrete promotion of open standards

All mechanisms outlined in this review can be strengthened through the promotion of OS software and open standards across governmental datasets and information assets. This means that they should be in standardised, machine-readable, non-proprietary formats. These characteristics are specifically referred to in guidelines, such as the Technology Code of Practice, Local Government Transparency Code, etc.

The limited practical support to local authorities means that applying the guidelines remains mostly an aspiration where it is likely to be most needed. Extending the support to local government offices, and increasing their technical and financial capacity, could offer practical routes towards promoting OS use in the development and purchase of ADM systems.

4. Freedom of information and subject access requests

Freedom of information (FOI) and subject access requests are one of the key tools used to surface information regarding ADM systems, as evidenced by much of the investigative work done in this area. A significant impediment to FOI disclosure is the exemption of commercially sensitive information.

6 Indeed, GDS Service Standard and the Service Manual could, in general, be used to promote transparency and accountability by clearly highlighting design solutions and practices that encode these principles.

A report published by the ICO last year notes that: 'Despite the fundamental role that private companies play as one of the major providers of public services, only 23% of the public we polled thought information about their activities was accessible.'

In the same report, the ICO has called for greater use of existing powers as well as legislative reform to enable contractors to be 'designated under Freedom of Information Act if they are providing a service that is a function of a public authority.' This is an important proposal to amplify given the Government's increasing reliance on private companies in public service delivery.

Takeaway 4: Extending the powers of FOI

The effectiveness of FOI requests in contributing to transparency on ADM systems in use in local and central government is significantly limited by the exemption of commercially sensitive information stated in the Freedom of Information Act, particularly relating to the role of private vendors in developing and implementing these systems.

Extending the powers of the Freedom of Information Act would contribute towards understanding how ADM systems currently in use operate.

5. Standardised disclosure of data used or produced in the deployment of ADM systems

Data-sharing agreements (DSAs):

Information or data-sharing agreements, which are responsibilities of Information Officers, offer some transparency for data-analytic processes. DSAs are usually established to initiate data sharing between authorities or departments that operate within different domains, or with external parties.

While DSAs have a variety of purposes – including for instance, research that uses depersonalised datasets, as authorised through the Research Strand of the Economy Act 2017 – the agreements that would be of interest in this context are those have a relationship to the implementation of ADM systems. The information that can be surfaced in DSAs focuses on the datasets being shared, the relationship between the sharing departments/institutions, the purposes of sharing as well as what is 'going to happen to the data at every stage'.

The Government maintains a register of data sharing agreements, with the Data Sharing Code of Practice stating: 'Information about all data sharing agreements under these powers should be submitted to the Government Digital Service (GDS) in the Cabinet Office who will maintain a searchable register available to the general public. The register will allow Government and the ICO to understand what data sharing is taking place under the provisions, to assess the value of the provisions, as well as run audits where appropriate and to check compliance with legislation, this Code and other security and data processing guidelines.'

Information asset lists and registers:

Under the Re-use of Public Sector Information Regulations 2005, authorities are expected to produce 'a list of the main information you hold within your public task'. This should include information that you already publish proactively and unpublished information.'

This mechanism can create significant visibility over the data used in support of the various forms of data processing carried out by government bodies, even if the datasets themselves are restricted. An example is the Home Office's information asset register.

Ensuring that this information is published in a standardised way across all authorities operating ADMs can make a significant contribution to transparency over these systems, and offer insights into the data-related functions of an organisation. Understanding the full scale and scope of the data-driven activities within government bodies can help better contextualise the role of ADM systems within governance activities.

Statistics:

The UK Statistics Authority's 'Code of Practice for Statistics' promotes the production of good-quality analytical outputs for any non-official statistics through a voluntary code of conduct. Public bodies also seek to maintain data quality through locally specified Data Quality Frameworks. These frameworks set data quality objectives and define data governance responsibilities to ensure good quality data is maintained to support decision making and service delivery.

The UK Statistics Authority also runs an issues log. Their website states: 'Inclusion in the list does not necessarily mean that the Authority shares the concern, nor does it indicate a commitment to further action by the Authority, although some of these matters will be followed up.'

These tools may also constitute a vehicle for publishing and raising issues around (or making proposals for) statistics to be collected on the decisions, categorisations and streaming choices made in the use of ADMs.

Takeaway 5: Standardising the disclosure of data used or produced while implementing ADM systems

DSAs, IA registers and statistical data can shed light on aspects of ADM systems, and the types of processing where it is not deemed appropriate to make public the source code or full datasets. They can help contextualise the function of ADM systems. Standardising and making available documentation on the data produced in support of ADMs in a systematic and intelligible way could make a significant contribution to the transparency of ADM systems.

Summary

The following table summarises how the questions listed at the beginning of this document can potentially be answered by one, or more, of the transparency mechanisms reviewed.

Transparency questions	Document / mechanism used	Is it public?	Is it mandatory? Is it enforced?
What are the data sources?	DPIAs, DSAs	Not usually	Some are technically mandatory but not strictly enforced
Who is operating the ADMs?	DPIAs, DSAs (for single owners responsible for the model/algorithm) contracts, procurement docs (for general info on responsible government department)	Single responsible owners usually are not, but info on government depts, private companies are often available	Some are mandatory but not strictly enforced
What is the purpose? What are the conditions around repurposing or use in other areas?	DPIA, DSA, procurement docs, audit trails, pilot reviews	Not usually	Some are mandatory but not strictly enforced
Why is the system being developed? What were the alternatives and how was the ADM system selected?	DPIA, DSA, procurement docs, audit trails	Not usually	Mandatory. Not strictly enforced.
What is the logic of the system?	Possibly DPIAs, source code, FoIs	Not usually	No
Who built it?	Contracts, procurement docs, audit trails, spending data (particularly if proprietary software) grey literature, Government reports, etc. (if developed in house)	Yes, but not centrally collected	Technically yes, but some not strictly enforced or standardised
How much did it cost?	Contracts, procurement docs, audit trails, spending data	Usually these documents are public, but are not centrally collected	Technically yes, but some not strictly enforced or standardised
What private actors are involved, if any?	Audit trails, local audit reports, procurement docs, spending data	Yes	Yes
What Government policies does it enact, if any?	Local audit reports, meeting minutes, audit trails (though none clearly define this), DPIAs usually mention this aspect	Some of them are public	Some of them are public
What are the impacts? Are specific groups impacted? Who are they, and how? What actions have been taken to mitigate risks? How are outcomes tracked?	IAs, pilot reviews, statistics	Not usually	No
What legal powers enable the use of the system?	Usually DPIAs	Not usually	Again, DPIAs are technically mandatory for high-risk data sharing and data-analytics applications, but are not always carried out.