COMMONWEALTH
OMBUDSMAN

Automated Decision-making

Better Practice Guide

Introduction

Automation plays a significant role in administrative decision-making. In the right areas and with appropriate management, automated systems can provide business benefits such as improved consistency, accuracy and transparency of administrative decision-making and new service delivery options.

Technological advances have made it easier for agencies to make automated decisions. However, it is well recognised that automated systems have the potential to significantly impact the rights and privacy of individuals. Agencies need to find a balance between innovation and ensuring automation is used only where appropriate.

The key message for agencies is that the customer must be at the centre of our service delivery.

Automated system design needs to recognise that at the end of a process or decision is a person who can be affected, positively or negatively. The same community expectations of respectful treatment and fairness apply to automated systems as they do when a decision is being made manually.

The structure of this guide reflects the areas that require particular care when developing and managing automated systems including:

1. **Guiding principles for assessing the suitability of automated systems.**
2. **Ensuring compliance with administrative law requirements.**
3. **Ensuring the design of an automated system complies with privacy requirements.**
4. **Establishing appropriate governance of automated systems projects.**
5. **Developing quality assurance processes to maintain continued accuracy.**
6. **Ensuring the transparency and accountability of the system and its accompanying processes.**

This guide is intended to be a practical tool for agencies and includes a checklist designed to assist managers and project officers during the design and implementation of new automated systems, and with ongoing assurance processes once a system is operational.

The principles in the guide apply whether an agency is building an automated system in-house or has contracted with an external provider to build the system. The use of external providers does not relieve agencies of the considerations identified in the guide or the risks that need to be managed. However, where external providers are used, the agency will also need to effectively manage the contract with the external provider.

Acknowledgements

This guide was originally published in February 2007 by a cross agency Working Group, building on the Administrative Review Council (ARC) Report No. 46 to the Attorney-General entitled Automated Assistance in Administrative Decision-making. The ARC Report contained 27 best practice principles for ensuring that automated assistance in decision-making is consistent with administrative law values.

This guide, updated in 2019 by the Commonwealth Ombudsman, the Office of the Australian Information Commissioner and the Attorney-General's Department, remains focussed on practical guidance for agencies aimed to ensure compliance with administrative law and privacy principles, and best practice administration. It draws on the experience of our agencies in overseeing the rollout of digital programs, and includes references to the complementary resources that have been developed since 2007. A number of other Commonwealth departments and agencies provided comments on the updated guide and we thank them for their assistance.

Any feedback on how the guide can be improved is welcome.

Contents

What is an automated system?

Automated systems range from traditional rules-based systems (for example a system which calculates a rate of payment in accordance with a formula set out in legislation) through to more specialised systems which use automated tools to predict and deliberate, including through the use of machine learning.

The term automated system is used in this guide to describe a computer system that automates part or all of an administrative decision-making process. The key feature of such systems is the use of pre-set logical parameters to perform actions, or make decision, without the direct involvement by a human being at the time of decision.

Automated systems can be used in different ways in administrative decision-making. For example:

- They can make a decision.
- They can recommend a decision to the decision-maker.
- They can guide a decision-maker through relevant facts, legislation and policy, closing off irrelevant paths as they go.
- They may include decision-support systems, such as useful commentary about relevant legislation, case law and policy for the decision-maker at relevant points in the decision-making process.
- They can provide preliminary assessments for individuals or internal decision-makers.
- They can automate aspects of the fact finding process which may influence subsequent decisions, for example by applying data:
  - from other sources (e.g. data matching information)
  - directly entered or uploaded to the system by an individual.

Guiding principles for automated systems

Automated systems must comply with administrative law principles of legality, fairness, rationality and transparency. They must also comply with privacy requirements and human rights obligations. As a matter of good public administration, they should be efficient, accessible, accurate and consider the needs of any vulnerable and non-digital ready users.

The legal frameworks of administrative law, privacy and human rights will assist agencies in designing automated systems to ensure that key risks in automation are avoided, such as algorithmic bias, inaccurate (or less accurate) decisions being produced by an automated system and unclear reasons for decisions.

Administrative law, privacy requirements and human rights obligations should be integrated into the design of an automated system through appropriate planning and assessment. The same principles apply when automated systems are reviewed by agencies.

Big data analytics, Artificial Intelligence (AI) and Machine Learning have become an increasingly utilised feature of automated systems. Agencies must also be mindful of the international standards relating to the use of AI. In May 2019, the Australia Government signed up to the Organisation for Economic Co-operation and Development Principles on Artificial Intelligence (the OECD AI principles). Under the OECD AI principles, an AI system is:

> a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. AI systems are designed to operate with varying levels of autonomy.[1]

In summary, the OECD AI principles state that:

1. 'AI should benefit people and the planet by driving inclusive growth, sustainable development and wellbeing.
2. AI systems should be designed in a way that respects the rule of law, human rights, democratic values and diversity, and they should include appropriate safeguards – for example, enabling human intervention where necessary – to ensure a fair and just society.
3. There should be transparency and responsible disclosure around AI systems to ensure that people understand when they are engaging with them and can challenge outcomes.
4. AI systems must function in a robust, secure and safe way throughout their lifetimes, and potential risks should be continually assessed and managed.
5. Organisations and individuals developing, deploying or operating AI systems should be held accountable for their proper functioning in line with the above principles.' [2]

1 / Organisation for Economic Co-operation and Development 'Recommendation of the Council on Artificial Intelligence' OECD/Legal/0449 adopted on 22 May 2019 accessed at https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449#_ga=2.201771153.1806885565.1559533436-1967103450.1558928769

In 2019, the Department of Industry, Innovation and Science released eight AI Ethics Principles, as part of a broader AI Ethics framework. A summary of the principles are:

1. **Human, social and environmental wellbeing**

   Throughout their lifecycle, AI systems should benefit individuals, society and the environment.

2. **Human-centred values**

   Throughout their lifecycle, AI systems should respect human rights, diversity, and the autonomy of individuals.

3. **Fairness**

   Throughout their lifecycle, AI systems should be inclusive and accessible, and should not involve or result in unfair discrimination against individuals, communities or groups.

4. **Privacy protection and security**

   Throughout their lifecycle, AI systems should respect and uphold privacy rights and data protection, and ensure the security of data.

5. **Reliability and safety**

   Throughout their lifecycle, AI systems should reliably operate in accordance with their intended purpose.

6. **Transparency and explainability**

   There should be transparency and responsible disclosure to ensure people know when they are being significantly impacted by an AI system, and can find out when an AI system is engaging with them.

7. **Contestability**

   When an AI system significantly impacts a person, community, group or environment, there should be a timely process to allow people to challenge the use or output of the AI system.

8. **Accountability**

   Those responsible for the different phases of the AI system lifecycle should be identifiable and accountable for the outcomes of the AI systems, and human oversight of AI systems should be enabled.[3]

The principles can be used throughout the lifecycle of AI and automated systems to achieve better outcomes, reduce the risk of negative impact and practice the highest standards of ethical business and good governance.[4]

The themes of these principles are discussed at different points throughout this guide as key features of automated systems.

[2] / Organisation for Economic Co-operation and Development, 'Forty-two countries adopt new OECD Principles on Artificial Intelligence' accessed at http://www.oecd.org/going-digital/forty-two-countries-adopt-new-oecd-principles-on-artificial-intelligence.htm

[3] / Department of Industry, Innovation and Science "AI Ethics Principles" accessed at https://www.industry.gov.au/data-and-publications/building-australias-artificial-intelligence-capability/ai-ethics-framework/ai-ethics-principles

[4] / Ibid

Is an automated system suitable?

Automation of any part of a process is not suitable where it would:

- Contravene administrative law requirements of legality, fairness, rationality and transparency.
- Contravene privacy, data security or other legal requirements (including human rights obligations).
- Compromise accuracy in decision-making.
- Significantly undermine public confidence in government administration.

This guide sets out some of the considerations when assessing the suitability of an automated system. Agencies should consider what steps they need to take in determining the suitability of an automated system depending on the possible impact of the decisions to be made by the automated system. For example, decisions that will have a significantly detrimental and irreversible impact on individuals will require more scrutiny compared to a decision with short term impact that is easily reversible.

The following checklist summarises some of the key considerations. A more detailed checklist is at Appendix A.

1. Assess whether system meets each of the AI Ethics Principles.
2. Assess whether the system will uphold the administrative law values of legality and fairness:
   i. Map whether the decision-making path involves the exercise of judgement or discretion.
   ii. Identify the legislative authority for the decision/s.
   iii. Identify whether notice is provided to an affected individual before a decision is made.
   iv. Consider consulting with an administrative law expert.
3. Engage a multidisciplinary team to assess the system:
   i. legal
   ii. policy owners
   iii. architecture, data and other information technology experts
   iv. program managers
   v. service delivery professionals.
4. Undertake a risk assessment.
5. Undertake a Privacy Impact Assessment.
6. Seek assurance from any contractors that legislative requirements and best practice principles have been adhered to.
7. Design and deliver according to Digital Service Standards.
8. Undertake testing and verification of rules to ensure decisions are legal, accurate, fair and consistent.
9. Undertake user testing of the system to ensure that the automated system and supporting channels are accessible and inclusive of people regardless of ability and environment.
10. Assess and deliver training needs for staff in using the system.
11. Ensure decisions can be easily explained to an individual or external oversight body, court or tribunal.
12. Provide publicly available information about the system.
13. Ensure there are avenues of review for decisions made.
14. Establish a sustainable and ongoing monitoring and review cycle to ensure decisions are legal, accurate, fair and consistent.

Administrative law and automated systems

Legislative authority for automated decisions

It is possible for an automated system to make decisions by using pre-programmed decision-making criteria without the use of human judgement at the point of decision. The authority for making such decisions will only be beyond doubt if specifically enabled by legislation. The construction of such an authorisation should nominate a position or title of a person with ultimate responsibility for the decision, such as the Secretary of the relevant department.

Discretion and automated systems

In 2004, the Administrative Review Council developed best practice principles for automated assistance in administrative decision-making. At that time, the Council was of the view that automated systems that make decisions, as opposed to helping a decision-maker make a decision, are generally only suitable for decisions involving non-discretionary elements.[5]

Automation of decisions is an evolving area, and there is not yet clear and definitive guidance from the courts about whether it is necessary for all discretions to be exercised personally by a decision-maker. For example, it is unclear:

- whether it is acceptable for discretions to be automated if they are set to apply beneficially to the person affected, or
- the extent to which a discretion may be automated (if at all) in circumstances where a person affected is:
  - provided with advance notice of the decision to be made and matters potentially adverse to their interests
  - permitted to make submissions regarding relevant matters of fact and law
  - able to ask for the decision to be made, or reviewed, by a human decision-maker.

Agencies considering automated systems for administrative decision-making must therefore pay particular attention to decision-making paths involving the exercise of judgement or discretion, to ensure that elements of decision-making involving the use of discretion or judgement uphold the administrative law values of legality and fairness.

What is discretion?

Discretion will generally exist in statutory provisions which:

- Provide the decision-maker with a range of options to choose between.
- Include words such as 'the decision-maker may' or ‘the Secretary may’.
- Require the decision-maker to exercise broad judgment where a statutory standard is to be applied, for instance, that the person is a 'fit and proper person' or concerning the ‘public interest’.
- Require the decision-maker to consider whether they have reached a ‘state of satisfaction’ that any legislative pre-conditions have been met before a decision is made.

Different outcomes can be reached in discretionary decisions, because different weight may be attached by the decision-maker to the relevant factors leading to a decision.

[5] Administrative Review Council, Automated Assistance in Administrative Decision Making, Report No 46 (2004)

There are inherent challenges in administering broad discretions, which can include additional cost and the risk of inconsistency in decision-making. However, discretions ensure legislative frameworks are sufficiently flexible. They are a tool to avoid unfair or unjust outcomes that might otherwise result from inflexible application of a particular statutory provision and can help ensure decision-making is consistent with broader legislative and policy intent. For example, a discretion to provide an exemption to a requirement, based on an individual's circumstances, can ensure hardship relief and fairness in administration of the statute.

Supporting discretionary decision-makers

When properly designed and modelled, automated systems may enhance the exercise of decision-making discretion and judgement by the following measures:

- only permitting the use of human discretion and judgement where it is relevant
- outlining and/or breaking down the factors decision-makers should consider when making their judgement
- providing links to relevant support materials and guides
- requiring that decision-makers clearly state and record reasons for decisions, as a statement of reasons or other official (and auditable) output.

Managing risks associated with discretions

The exercise of discretion and judgement in the administrative decision-making process does not itself preclude automation of the business process within which a discretionary consideration must be made. However, agencies must ensure that the legality and fairness of discretionary administrative decisions are preserved when automating the decision-making process.

This means close and ongoing liaison with administrative law experts is critical where decisions, especially those involving discretions, are being considered for automation. This includes seeking expert external legal advice where necessary.

An automated system must be designed in a way that complies with the legislative framework which confers authority to make a discretionary decision and accurately reflects the government policy it models. Agencies should be particularly careful that the system does not constrain the decision-maker in exercising any discretion he or she has been given (under relevant legislation, policy or procedure) or lead to a failure to consider relevant matters which are expressly or impliedly required to by the statute.

An automated system that builds on or around an administrative decision-making process and requires agency officers to exercise discretion or judgement should expressly advise the decision-maker that the question being asked is a matter for the decision-maker's judgement.

Agencies should also ensure that automated systems' business rules relating to discretion and judgement, and any research linked to the use of discretion and judgement, are readily and openly available, and subject to internal and external review.

Discretionary decisions based on data input from the person affected by the decision must include clear, relevant and accessible guidance for the user (e.g. pop up messages, warnings and commentary inbuilt into the automated system) to assist the person to input the data required.

Agencies should ensure the system enables recording and archiving the decision-maker's deliberations or reasoning on matters of discretion or judgement and ensure that these are accessible and comprehensible for the purposes of internal and external review.[6]

Agencies should ensure that reasons for the decision and review pathways are clearly and effectively communicated to the person affected by the decision.

[6] / The advantage of such a facility is that the audit trail will include the points of the decision-making path where discretion or judgement matters are decided and the reasons for making such judgements. This facilitates not only internal and external review and audit, but also enables deliberations to be incorporated into any notification of decision or statement of reasons that the client or customer of the agency receives.

Privacy

Where privacy risks are anticipated, they can be adequately managed as part of the automated system's design.

Agencies developing or redeveloping automated systems that involve the collection, use or storage of personal information should consider how the design of the system (and its business processes) will protect the privacy of an individual's personal information. As a general rule, when designing business or workflow rules for automated systems, agencies should look for and choose the least privacy-invasive method that also meets their business needs.

Agencies should always refer to the *Privacy Act 1988* (Cth) (Privacy Act) for a comprehensive understanding of their privacy obligations. Under the Privacy (Australian Government Agencies – Governance) APP Code 2017 all agencies subject to the Privacy Act must undertake a written Privacy Impact Assessment (PIA)[7] for all 'high privacy risk' projects or initiatives that involve new or changed ways of handling personal information. This will likely include automated decision-making projects which utilise personal information handled by agencies.

Privacy by design[8] and PIAs should form part of an agency's regular risk management and planning processes when an entity is developing or reviewing a project that uses automated decision-making.

Agencies should refer to the Office of the Australian Information Commissioner's (OAIC) website at oaic.gov.au for more information and guidance.

The Privacy Act 1988 (Cth)

The Privacy Act contains 13 Australian Privacy Principles (APPs) which apply to some private sector organisations, as well as most Australian Government agencies.

The APPs govern the standards, rights and obligations around:

- the collection, use and disclosure of personal information
- an organisation or agency's governance and accountability
- integrity and correction of personal information
- the rights of individuals to access their personal information.

The APPs are principles-based law. While the APPs are not prescriptive, each agency needs to consider how the principles apply to its own situation. A breach of an APP is an 'interference with the privacy of an individual' and can lead to regulatory action and penalties.

Agencies should also consult the OAIC's APP guidelines, which outline the mandatory requirements of the APPs, how the OAIC will interpret the APPs, and matters the OAIC may take into account when exercising functions and powers under the Privacy Act.

If agencies use contractors as part of their automated decision-making projects they will also need to comply with s 95B of the Privacy Act, which requires agencies to take contractual measures to ensure that a contracted service provider does not do an act, or engage in a practice, that would breach an APP if done by the agency.

[7] A PIA is a systematic assessment of a project that identifies the impacts that the project might have on the privacy of individuals, and sets out recommendations for managing, minimising, or eliminating that impact.

[8] Privacy-by-design is a holistic approach where privacy is integrated and embedded in an agency's culture, practices and processes, systems and initiatives from the design stage onwards. This includes taking a risk management approach to identifying privacy risks and mitigating those risks.

[9] Schedule 1, Privacy Act recommendations for managing, minimising, or eliminating that impact.

What is personal information?

'Personal information'[10] includes a broad range of information, or an opinion, that could identify an individual. What is personal information will vary, depending on whether the person can be identified or is reasonably identifiable in the circumstances.[11] For example, personal information may include:

- an individual's name, signature, address, phone number or date of birth
- sensitive information (discussed below)
- credit information
- photographs
- internet protocol (IP) addresses.

'Sensitive information', which generally has a higher level of privacy protection, is personal information that includes information or an opinion about an individual's:

- racial or ethnic origin
- political opinions or associations
- religious or philosophical beliefs
- trade union membership or associations
- sexual orientation or practices
- criminal record
- health or genetic information
- biometric information

When conducting automated decision-making, agencies should remember that personal information includes opinions or inferences drawn about people from other data, whether or not these are accurate. This is especially pertinent when automated decision-making is informed by sophisticated analytics or algorithms, involving artificial intelligence and machine learning.

Australian Privacy Principles and automated decision-making

The following part of the guidance takes you through a selection of APPs that are particularly relevant to automated decision-making and outlines the factors to consider when undertaking any projects involving automated decision-making.

See the OAIC's Australian Privacy Principles guidelines[12] for further detail on the APPs.

Be open and transparent (APP 1)

The objective of APP 1 is to ensure agencies manage personal information in an open and transparent way. By complying with this APP your agency will be establishing a culture and set of processes that will assist you in complying with all the other APPs, right from the start.

APP 1 does this by requiring agencies to take reasonable steps to establish and maintain internal practices, procedures and systems that ensure compliance with the APPs (APP 1.2) and, by requiring agencies to have a clearly expressed and up to date APP Privacy Policy describing how it manages personal information (required by APP 1.3).

Australian Government agencies should also be aware that they also have specific obligations under APP 1.2 as set out in the Privacy (Australian Government Agencies – Governance) APP Code 2017 (Privacy Code). Guidance on the Privacy Code is available on the OAIC's website.

[10] / See subsection 6(1) of the Privacy Act for the definitions of 'personal information' and 'sensitive information'.

[11] / For more information refer to the OAIC's 'What is personal information?' guidance, available at https://www.oaic.gov.au/privacy/guidance-and-advice/what-is-personal-information/.

[12] / https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/

The complexity of automated decision-making projects can mean that the processing behind them is opaque to the individuals whose data is being used. It may not be apparent to them their data is being collected, or how. Despite the challenges, with planning and foresight, transparency and good privacy governance in relation to automated decision-making can be achieved. Being open and transparent about how your agency will handle personal information will help to ensure that you have a culture that respects and protects personal information. It also plays a key role in building public and consumer trust, improving outcomes from automated decision-making, and encouraging innovation.

Collect only what is reasonably necessary (APP 3)

APP 3 outlines when personal information, including sensitive information, may be solicited and collected by agencies. It places obligations on agencies to:

- collect personal information only where it is reasonably necessary for, or directly related to, the agency's functions or activities
- collect information only by legal and fair means
- collect information directly from the individual, unless it is unreasonable or impractical (or another exception apples)
- collect sensitive information only where:
    - the collection of the sensitive information is reasonably necessary for or directly related to one or more of the agency's functions or activities
    - the individual concerned consents to the collection.

Taken together, the requirements in APP 3 seek to strike a balance between the interests of automated decision-making projects and the privacy of individuals. Personal information collected by an agency may generally be used or disclosed only for the primary (original) purpose for which it was collected, unless the individual consents or another exception applies (APP 6, discussed further below).

This means the way personal information is collected, and the notice given to the individual concerned, is key when conducting automated decision-making, as it will in part determine the scope of how the information can be used (APP 5, discussed further below).

More information about collecting personal information is provided in Chapter 3 of the APP Guidelines.

Agencies using automated systems for self-assessment (at a shopfront, via the internet, or at interview) may find that information and data entered by a self-assessing user may not need to be stored by the system, thereby reducing the privacy risks and security requirements associated with use of a system.

Give notice to individuals about how their personal information will be handled when you collect it (APP 5)

When your agency collects personal information, APP 5 requires that reasonable steps be taken to either notify the individual of certain matters, or to ensure the individual is aware of those matters. These matters include:

- the agency's identity and contact details
- the fact and circumstances of collection
- whether the collection is required or authorised by law
- the purposes of collection
- the consequences if personal information is not collected
- the agency's usual disclosures of personal information of the kind collected by the entity
- information about the agency's APP Privacy Policy
- whether the agency is likely to disclose personal information to overseas recipients, and if practicable, the countries where they are located.

An agency must take these steps before or at the time it collects the information. If this is not practicable, reasonable steps must be taken as soon as practicable after collection.

Providing notice effectively can be challenging for automated decision-making. Nevertheless, agencies still need to give individuals notification of the collection of their data. Privacy notices, therefore, need to communicate information handling practices clearly and simply but with enough detail to be meaningful. Innovative approaches to privacy notices can include 'just-in-time' notices (appearing on the individual's screen at the point where they input personal data, providing a brief message explaining how the information they are about to provide will be used), video notices and privacy dashboards.

Use or disclosure for an authorised purpose (APP 6)

APP 6 outlines when an agency may use or disclose personal information. It provides that personal information may only be used or disclosed for the purpose for which it was collected (known as the 'primary purpose'), or for a secondary purpose if an exception applies. This principle may appear to present a challenge when conducting automated decision-making, as the ability to analyse data for different purposes is an important characteristic of automated decision-making.

Depending on the application, automated systems can become (or be integrated with) information-rich databases of personal information. Information-rich data bases, particularly those containing sensitive information, may be valuable to other agencies, including law enforcement agencies, and are sometimes the subject of unsolicited requests for information, or for formal approaches for data-linking. In practice, your agency will need to be able to determine whether the uses and disclosures of personal information to a third party are compatible with the original purpose it was collected for, and the privacy policy and/or notice given to the individual. If the use or disclosure of personal information is not compatible with the primary purpose, you will need to rely on one of the exceptions set out in APP 6 in order to disclose such data.

The business practices overarching an automated system should minimise the risk of individuals being surprised as to how their personal information has been handled. You may choose to update your privacy policy and notices accordingly, ensuring that people are aware of likely secondary uses and disclosures of personal information (including automated decision-making projects). This may help to establish that an individual would likely expect the use or disclosure, or in some cases help to establish that an individual has provided informed consent[13] to the use or disclosure of their information for a secondary purpose. Agencies should also consider how they might allow individuals to genuinely choose which uses and disclosures they agree to and which they do not.

More information about use and disclosure is provided in Chapter 6 of the APP Guidelines.

The proposed automation of some administrative processes is sometimes contingent upon linking existing electronic data sources to a new automated system. Where personal information is to be populated from other sources (and the data to be used within an automated system was initially collected for a different purpose), it is essential to ensure that use of existing electronic data is permitted under the Privacy Act.

[13] For more information on bundled consent see paragraphs B.45-B.46, OAIC's Australian Privacy Principles Guidelines: https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-b-key-concepts/

Information used for decision-making must be accurate, up-to-date and complete (APP 10)

Administrative law requires that decisions must be based on reliable and relevant information. The Privacy Act complements this requirement by requiring agencies to take reasonable steps to ensure that the personal information they collect is accurate, up-to-date and complete (APP 10.1). Similarly, agencies must take reasonable steps to ensure that the personal information it uses or discloses, having regard to the purpose of the use or disclosure, is accurate, up-to-date, complete and relevant. Guidance about the meaning of the terms 'accurate', 'up-to-date', 'complete' and 'relevant' is provided in Chapter 10 of the APP Guidelines.

Large scale automated decision-making supported or underpinned by data analytics, AI and machine learning may appear to present some challenges to the principles of accuracy and relevance of data. For example, these activities typically seek to collect large amounts of data from many diverse sources, with limited opportunity to verify the relevance or accuracy of the information. Further, some data analytics techniques that support automatic decision-making such as automatic algorithms have the potential to create personal information with an inherent bias, that is discriminatory or that leads to inaccurate or unjustified results.

Ensuring accuracy and quality in data analytics is particularly important where information may be used to make decisions about an individual, such as an administrative decision by a government agency. In these situations, it would be prudent for agencies to take rigorous steps to ensure the quality of both the personal information collected, as well as any additional personal information created by the algorithms that process the data. For example, consider conducting regular reviews of your data analytics processes (such as algorithms used), to ensure that they are fit for purpose and promote the accuracy of information.

Agencies should make automated and manual compliance intervention processes as easy as possible for customers to understand and use. Agencies should be as transparent as possible about the purpose of their analytic techniques (including algorithms), to better help individuals understand why automated decisions have been made about them. An internal document may be more appropriate for commercially sensitive techniques.

Agencies should have data validation processes in place before using personal information to inform automated decision-making. Where possible and appropriate, verify the accuracy of information which is not collected directly from the individual. For example, checking that third parties from which personal information is collected have implemented appropriate practices, procedures and systems to ensure the quality of personal information. It may also be useful to put in place procedures to monitor and record what type of personal information you are collecting.

Specific information risks that can arise include:

- an automated system might inappropriately incorporate unrelated, unchecked, unstable, outdated or unreliable data (for example from third parties) which can enter the decision-making pathway without the data flaw being identified or critically examined by an officer. This is a particular risk with pre-populated fields sourced from previously collected information
- an automated system might automatically generate or calculate new personal information (data, opinions or decisions) for use in decision-making about an individual, but for which the level of reliability or accuracy of the information is not obvious to the decision-maker.

An automated system's design should identify the types of personal information that are (a) subject to change or potentially unreliable, and (b) relevant to the making of a decision. The resultant workflow should prompt for updated information to be obtained prior to a decision being made.

Secure handling of personal information (APP 11)

APP 11 requires agencies to take reasonable steps to protect personal information from misuse, interference and loss, as well as unauthorised access, modification or disclosure. Guidance on the terms 'misuse', 'interference', 'loss', 'unauthorised access', 'unauthorised modification' and 'unauthorised disclosure' is provided in Chapter 11 of the APP Guidelines.

Automated system projects can be accompanied by the creation of information-rich data stores. Centralising or connecting previously disparate or unconnected data sources (for example, interview records and databases), can make personal information potentially more susceptible to unauthorised access, modification or disclosure, particularly when the data is stored in a consolidated way (a 'honey pot').

Agencies need to consider what security risks exist and take reasonable steps to protect the personal information they hold. This includes internal and external risks. It is expected that agencies handling large amounts of personal information as part of automated decision-making will conduct an information security risk assessment (also known as a threat risk assessment) as well as undertaking a PIA.

Undertaking an information security risk assessment will assist the entity to identify reasonable steps to take to protect personal information. Information about reasonable steps, including examples of what may be reasonable steps, is provided in the OAIC's Guide to securing personal information.

Agencies should have a response plan for potential data breaches that includes procedures and clear lines of authority, which can assist an entity to contain the breach and manage their response. The OAIC's Guide to managing data breaches in accordance with the Privacy Act 1988 provides guidance for organisations when responding to a data breach involving personal information. In the event of a data breach, agencies should also consider whether the nature of the breach dictates that they need to notify the OAIC under the Notifiable Data Breaches scheme.

Governance and design

Automated systems projects must establish appropriate governance frameworks and ensure that legal, policy and program areas are involved during the system's development.

In developing automated systems projects, agencies should apply high standard information technology project methodologies and techniques and the Digital Service Standard[14]. Additionally, the Australian Government privacy framework requires agencies have privacy project planning and governance mechanisms in place. The above section deals comprehensively with privacy requirements.

Enabling scrutiny of the development of an automated system is as important as the transparency and accountability characteristics of the system itself. Whatever governance arrangements are appropriate to the project and the agency environment, agencies should ensure that project decisions regarding automated systems and/or exercise of discretion or judgement are adequately documented.

There are potentially many inputs to the decision as to which areas are suitable for automated decision-making. Scoping for an automated system project should include an examination of the relevant legislation, policies or procedures, and the specific clauses and/or parts that an agency seeks to automate.

Authorised decision-making

As authority to act is a fundamental tenet of administrative decision-making, it is important that the verification process for an automated system is able to test whether the nominated decision-maker is authorised to act. As a consequence, the audit facility should be able to report user access and decisions against delegations.

Verification and quality assurance processes are particularly important where a decision-maker is exercising delegations under multiple Acts, on behalf of another agency or under contract. In these instances, an automated system should be designed to allow functionality privileges or access commensurate with users' delegations. Quality assurance is addressed further below.

Any approach taken to deal with discretion or judgement within an automated system should have the capacity to capture and record the decision-maker's reasoning. This capacity should preferably be built into the system itself, to ensure that the automated system's audit trail clearly sets out each of the decision points involving discretion or judgement.

[14] https://www.dta.gov.au/help-and-advice/about-digital-service-standard

The importance of multidisciplinary teams

Automated systems projects need to draw on diverse skills to be most effective. This is necessary to safeguard against unintentional outcomes and to ensure legislative compliance. Typical projects include skills and expertise from a wide range of areas—including the business areas (e.g. legal, policy, work practice and program areas) and information technology areas of the agency (such as business analysts, systems development specialists, testing and integration).

Teams should also include people with implementation and service delivery expertise (such as those in customer-facing or call centre roles) as well as users of the product or system to ensure that usability issues and acceptance of the system are considered from the outset of the project[15].

A documented verification strategy is essential if an agency is to have confidence in the accuracy, consistency and currency of its automated system. For a verification strategy to be effective, it must be incorporated into the governance framework for the automated system project, and must link with the policy ownership strategy.

The verification strategy should ensure that the following project stakeholders are consulted internally and externally where necessary:

- legal
- policy owners
- architecture, data and other information technology experts
- program managers
- service delivery professionals.

Interfacing an automated system with other agency systems can prove difficult due to the existence of different data definitions, existing services and different processing hand-offs. The total information technology solution, of which an automated system may be only one part,could consist of a mixture of business rules and procedural code, which should be understood at the outset.

Application of Digital Service Standard

The Digital Transformation Agency's (DTA) Digital Service Standard (the Standard) is a set of best-practice principles for designing and delivering government services. Agencies should refer to the guidance on the DTA's website dta.gov.au on how to meet the Standard.

The Digital Service Standard is mandated for Australian Government services that are:

- public facing
- owned by non-corporate Commonwealth entities
- new informational or transactional services (designed or redesigned after 6 May 2016)
- existing high-volume transactional services.

This Guide summarises some of the key considerations relating to user needs, testing and data security in the design of an automated system.

[15] / See Criterion 2 of the Digital Service Standard – Have a multidisciplinary team

User needs

In line with the government's digital transformation agenda, agencies are increasingly delivering online services which involve members of the community directly inputting data to automated systems. Where this is the case, the accuracy of automated decisions relies, at least in part, on the accuracy of the data entered by the user. While it is the individual's responsibility to answer the questions correctly, it is important for agencies to provide sufficient guidance to ensure:

- the user understands from the outset what the process will require from them, including what information they will need to have to hand
- where they have options or choices about how to use the process or service, guidance about which option is appropriate for them, and the consequences of their choices
- where to go for help if they have difficulties or questions.

The automated system and supporting channels must be accessible and inclusive of everyone regardless of ability and environment. This includes people with disability and older people, and people who cannot use or struggle with digital services. This may mean providing access to non-online channels as well as online access to the system.

Where the user has an option not to engage with an automated system at all, but not engaging may result in an adverse decision, clear and effective communication is essential about how to engage, why to engage, what will happen if they do not engage and how to access support.[16]

Support in using the automated system should be readily accessible, and include non-online channels (e.g. telephone lines). Special consideration and support should be given to vulnerable people, including those with disability, older people and people in rural and remote Australia.

Systems should be designed so that staff supporting users are able to see the same system as the user. Consideration should also be given to how community groups may be permitted to use or see an automated system for the purpose of providing assistance to individuals or particular user groups.

Testing

Automated systems are improved by external perspectives. Wherever possible, systems should be tested with a broad range of real users, service delivery staff, oversight agencies and other organisations that support users in the design and delivery stages.

Stakeholder input into an automated system project might include:

- reviewing interview or categorisation questions
- verifying business rules relating to contested interpretations of the law
- providing scenarios designed to test the limits of a system
- granting access to system training or a test environment.

A verification strategy might also include inviting feedback on the accountability features of an automated system for the purposes of ensuring accuracy. Again, for external verification to occur, the underlying business rules contained in an automated system should be accessible and in a readily understandable form.

[16] See, for example, recommendations 2,3 and 5 in Commonwealth Ombudsman's report Centrelink's automated debt raising and recovery system, April 2017.

Data security

Agencies should adopt suitable procedures for accurately collecting and safely storing data used by automated systems. Data security must be part of the design beginning with identification of the data and information the system will use or create. Agencies need to ensure the automated system complies with all legal and policy requirements including the data security framework of the agency.

The DTA provides guidance for agencies on data security requirements throughout the design phases through to implementation.

Agencies need to understand their obligations under the following Australian Government frameworks:

- Information Security Manual
- Protective Security Policy Framework
- Information Security Registered Assessors Program Assessment.

In addition to privacy requirements which are covered in the above section, agencies may need to be aware of requirements relating to:

- records management
- the *Freedom of Information Act 1982* (Cth)
- the *Spam Act 2003* (Cth)
- any state and territory government policies.

Modelling and approval of business rules

In the same way that manual administrative decision-making processes must ensure the ongoing accuracy of decisions, particularly as legislation, policy and procedure change, automated systems must also have processes in place to ensure that the system is producing accurate decisions which comply with the legislative framework. The accuracy of an automated system is of paramount importance in ensuring compliance with the administrative law values of legality and rationality.

Modelling the business rules

In law, legislation prevails over policy. Neither policy nor procedures can be incompatible with legislation—to be so would cause an agency to act outside of the legal authority provided to it by the Parliament.

Developing an automated system will often begin with an analysis of business needs and practices derived from the legislation, policy and procedure. This leads to the documentation of a comprehensive set of business rules.

Each rule needs to be authorised by legislation, and supported by settled policy and/or procedures. For accountability reasons, a verification process should be followed.

The business rules used by automated systems for administrative decision-making should also closely mirror the structure of the legislative or policy sources. This strategy avoids unnecessary and undesirable interpretation of the source material that may lead to misinterpretations.

Mimicking the structure as well as the detail of relevant legislation, policy or procedures also allows for manual comparisons to be made of both the rules and the source, enabling the authenticity of the rules to be checked or verified.

Another strategy is to reference each business rule in an automated system with the relevant citation of the source from which it was derived, for example, the particular section or subsection of the Act or the paragraph in the policy or work practice manual. This is important so that each rule's lineage can be verified. This strategy also makes it easier for an automated system to be maintained when legislation, policy or procedures change.

It is essential that the business rules modelling process accurately captures legislative and policy provisions as well as the relevant procedures. It should not narrow the scope, application, context or meaning of the enabling legislation, nor reinterpret the policy objective.

Sometimes the 'modelling' or 'rules definition' process will reveal inconsistencies in the way legislation, policy or procedure may have been administered. It may also expose anomalies in the legislation, policy or procedure itself. In each case, to aid accountability, the anomaly or inconsistency should be settled within the governance process.

Business process mapping between systems

Where inputs or outputs of the decision-making process involve tasks and/or processes that are undertaken by other agency IT systems, it is important that these processes (and the timeframes and dependencies between systems) are clearly understood during development of the automated system.

Agencies may find that mapping the business processes between systems during the design phase is useful, both for the management of integration with other IT systems and for the design of the automated system itself.

Business rules update

Automated systems should be designed so that changes in the business rules can be easily updated across systems, and do not require major rework at each system interface.

Technical solutions should be found that maximise the interoperability of the automated system interface (with other IT systems), and therefore minimise the cost, time and disruption caused by the update process.

Data mapping to terms and definitions

Where automated systems integrate with existing IT systems, time should be taken to ensure that the data mapping of terms and definitions (relating to the agency's administration of the program area) in existing IT systems is interoperable with the data mapping and definitions in the automated system.

Consistent data mapping is of particular importance when information and data are drawn from other agency IT systems (such as databases or case management systems) into the automated system, or vice versa. If the definition and data mapping of facts relevant to an administrative decision (for example, 'spouse' or 'income') is considered and agreed upon early, considerable time and complexity can be avoided later in the project.

Consultation on this issue is advised during the analysis of the project, and should involve (at a minimum) the policy owners of the project and the relevant agency data and information management professionals.

Where possible, agencies should undertake a data 'harmonisation' process, identifying common elements, eliminating duplicate data and mapping to an agreed taxonomy (preferably using an international or other agreed data standard).

Implications for maintenance

During the design phase, agencies should consider how best to build an automated system having regard to future maintenance requirements.

Maintenance and update of the business rules will be an ongoing task for most automated systems. The update process is a vital determinant of the accuracy of the decisions made by an automated system. Depending on the complexity and frequency of legislative, policy or procedural change, updating could involve only simple changes in various fields, or the incorporation of large sets of new or changed business rules into the system. Agencies should be aware that the technical design of a system, its integration with other IT systems and the ease of access to and update of each individual business rule will have major implications for the time, costs and efficacy of the maintenance procedures and processes of the automated system.

Versioning

Automated systems used for administrative decision-making should be able to maintain and execute different versions of the business rules where required. This is particularly important where legislation, policy and procedure (and, subsequently, the business rules of an automated system) change, and the underlying administrative or legal process requires an agency to process backdated decisions (which may require the application of an earlier version of the business rules).

Agencies should be aware of the importance of versioning during the design process, and consult the relevant underlying legislation, policy and/or procedures to ensure that there is a clear understanding (e.g. among the policy owners of the system) of the legal and administrative obligations for the backdating of administrative decisions.

Where the processing of backdated decisions is required via an automated system, the system may require the capability to access and execute an earlier version of the business rules at a given point in time (as determined by the dates of changes to legislation, policy or procedure).

Quality assurance

Quality assurance can be used to test the intuitiveness of an automated system. It is important to understand whether a shortcoming in the system design (e.g. the imprecise structure of questions or answer categories) might contribute to an error or make a system unreliable in some respects.

Quality assurance may also point to areas where training could be better targeted, or identify how else the system might support better administrative decision-making.

In addition, an automated system needs to have a comprehensive audit trail to recall each decision point for analysis, to enable quality assurance testing of the system.

System monitoring and testing

It is vital that agencies using an automated system for administrative decision-making have robust processes for testing the system, both during its development and following its implementation. Testing of the system should commence from first principle (i.e. from the first level of legislative rules), occur each time a modification to the system is made, and provide an ongoing monitoring cycle of the appropriateness of the decision-making carried out throughout the life of the system.

Accurate collection of information

When designing a user interface for members of the public or for staff, agencies need to be alert to the potential for questions, fields and labels within an automated system to favour, or select for, one type of response over another. Narrowly expressed questions, fields or labels, or incomplete business rules might artificially limit the effectiveness of the information gathering process that is essential to good administrative decision-making and is also a key privacy concern.

Poorly expressed fields or questions present the risk that a decision will be made without sufficient information, and without an awareness that further information is required for a reasonable decision-making process to occur. The questions, fields or labels a user sees when using an automated system should be derived directly from the underlying business rules of the system, which are in turn also derived from the relevant provisions of the relevant legislation, policy or procedures.

Staff training

Implementation gaps can arise between the design of an automated system and the way users use it. Concepts and issues that may be obvious to an expert group may be obscure or not understood by users.

The verification strategy should ensure that the policy owner retains input into the analysis of the training needs of users (for example via pre- and post-decision quality assurance processes). Where warranted, the policy owner might also be involved in training delivery to reinforce the policy intention with user.

New roles may require development of more specific skills, for example in customer service, specialised interviewing skills or systems verification and quality assurance. Regardless of the skills and training mix the changed business processes demand, agencies should ensure that they have identified and addressed training requirements upon implementation of the automated system, including adequate provision for ongoing officer training.

Training requirements will vary depending on the nature of the decision being made. In all cases, staff must be able to adequately explain a decision made by an automated system or identify an appropriate escalation path for a customer seeking information.

Data quality

The data collected and used by the automated system must be accurate, complete and compliant with policy and legislative requirements relating to privacy and information management.

Agencies should adopt suitable procedures for accurately collecting and safely storing data used by automated systems in administrative decision-making. Particular consideration needs to be given to data quality in self-assessment systems, as these systems rely upon the manual collection and entry of data.

Where external data inputs are used e.g. data from a third party, consideration needs to be given to providing an opportunity for customers to dispute the accuracy of that data.

Data quality not only encompasses the requirement that agencies use suitable practices for the collection and storage of data at the outset of their administrative processes, but also that steps are taken to ensure the accuracy and security of this data over time. This might mean that agencies also consider the potential impact on data quality of any software or hardware changes to automated systems, and reconfirm that a system's operations still match the current business rules.

One strategy to ensure data quality, might be to consider the way in which automated systems are included in business continuity management plans, and to ensure the ongoing reliability and integrity of these systems.

Business continuity

Agencies should ensure that interim strategies are in place in the event that the system fails, or an update cannot be made immediately.

When errors in the system cannot be fixed immediately, management-initiated 'workarounds' can be developed, whereby officers are advised of the problem and given instructions for remedying it. In this regard, 'alerts' can be placed in the system as soon as the policy change occurs. These alerts can notify decision-makers that the business rules might have changed and those parts of the system can be 'turned off'.

Business continuity management arrangements should be in place to ensure that, when required, an appropriately trained officer can make a decision manually and explain this decision to an applicant.

Design principles for comprehensive audit trails

An audit trail is an essential part of a successful automated system design. To have a majority of desirable attributes present in a comprehensive electronic audit trail, agencies should consider applying the following good design principles:

- Have you designed the audit trail to include clearly identifiable links to authorised delegations (at every stage of the process)?
- Does the audit trail feature in the agency's design for automated systems?
- Will the audit trail's design meet the agency's business requirements, internal controls, transparency and accountability criteria, and audit requirements?
- Will the audit trail's design provide for archiving and continuity of access? Have you considered how change control processes will be reflected in the audit trail:
  - to record modifications to the system's operation or performance?
  - to reflect changes to the legislation that underpins the operation of the system?

Transparency and accountability

The underlying business rules of an automated system must be readily understandable and information about automated systems should be publicly available.

Publicly available information

The *Freedom of Information Act 1982* (FOI Act) is the legislative basis for open government in Australia and covers Australian Government ministers and most agencies. Under the FOI Act, most agencies have obligations to publish operational information as part of their Information Publication Scheme.[17] Operational information is information held by the agency to assist the agency to perform or exercise the agency's functions or powers in making decisions or recommendations affecting members of the public (or any particular person or entity, or class of persons or entities).[18] Examples include the agency's rules, guidelines, practices and precedents relating to those decisions and recommendations.

The OAIC has also developed principles on open public sector information which form part of a core vision for government information management in Australia and sit alongside the FOI Act.

Transparency and public access to government information are important in their own right and can bolster democratic government. Information sharing better enables the community to contribute to policy formulation, assist government regulation, participate in program administration, provide evidence to support decision-making and evaluate service delivery performance. A free flow of information between government, business and the community can also stimulate innovation to the economic and social advantage of the nation.

Agencies should seek advice about their requirements under the FOI Act, *Privacy Act 1988*, *Archives Act 1983* and open access to information responsibilities.

Websites are the main way that agencies communicate with the public and provide an opportunity for agencies to publish simple information about the use of automated systems.

Rules to be verified

It should be noted that disclosure of the business rules does not fully resolve the issue of whether the underlying coding has correctly implemented each business rule and its interaction with other rules. The most practical way to check this is for an agency to have a robust verification strategy, in which the policy area actively participates in test cases.

Automated systems should be understandable

Automated systems should be designed with disclosure and external scrutiny in mind including:

- who made the decision
- under what authority
- how the decision was made.

This is essential for agencies to comply with their legal and accountability obligations. While it is possible to trace coding back to its origin, what agencies need to be able to do is to demonstrate in a non-technical way how the decision made was legal, fair and can be perceived to be fair.

[17] Section 8(2)(j) Freedom of Information Act 1982

[18] Ibid s 8A

Audit

Disclosure and exposure to audit are important expressions of the transparency and accountability policy of government, and contribute significantly to confidence in public administration.

To ensure that the appropriate law, policy and procedure have been correctly applied to individual circumstances, an automated system should be able to automatically generate a comprehensive audit trail of the decision-making path.

The audit trail should be derived from the underlying business rules of the automated system, and the interaction between the rules and the facts of the case. In some cases, this enables the decision-maker to check or review the determination made via the automated system before finalising the decision. It also enables external scrutiny of the administrative decision.

Statement of reasons

Giving reasons for decisions is a fundamental requirement of good administrative decision-making. Where the audit trail is incorporated into a statement of reasons (or a notice of decision), it enables individuals or entities affected by decisions to understand the basis of those decisions. A statement of reasons needs to be in plain English and should be designed in a way that facilitates a meaningful understanding of the basis for the decision.

It may not be sufficient for an automated system to simply generate a printout of the outcome of the decision-making process.

A statement of reasons would typically:

- Set out the decision (what has been decided).
- List findings on material questions of fact and include a probative assessment or weighing of evidence.
- Include a statement about why the decision is preferred over other available alternatives (and cite the relevant authority or precedent, where applicable).
- Demonstrate that the decision is within power (i.e. jurisdiction) and that an appropriate test provided for in legislation has been used.
- List any avenues that are open to a person to challenge or appeal the decision.

It is not necessary for a statement of reasons to include every detail of the decision-making path. For example, if part of the decision includes complex calculations that are based on a formula set out in the legislation, it may not add to an individual's understanding of a decision for the complex calculation to be set out in a decision letter. However, all elements of the calculations should be exposed in an audit trail and be available upon request. This capability would also allow for more effective internal quality assurance and external review.

It is important that the audit trail of an automated system is not able to be altered or manipulated by users (so that the integrity of the audit trail is not compromised). However, it is practical to allow decision-makers to edit statements of reasons to make them fit for the purpose (e.g. to make them more likely to be understood by the recipient).

Review of decisions

Customers must be provided with an opportunity to dispute an administrative decision made by or with the assistance of an automated system. Many administrative decisions are subject to a legislative review process. In other cases, the agency should offer an option for internal review by a staff member as a part of a commitment to fair and reasonable decision-making. External avenues of review should also be provided to customers such as the option to make a complaint to the Ombudsman or taking a matter to a tribunal or court.

Monitoring and evaluation

Agencies should monitor and evaluate the automated system on an ongoing basis. Consideration should be given to data sets such as complaints data that will inform the agency about how the automated system is operating.

Agencies planning the monitoring and evaluation cycle need to establish early:

- The frequency and level of information required to determine benefits realisation at, or before, implementation of the system.
- Agreement on the specific data sources and information to be monitored and reviewed, and on a schedule for assessment and reporting of these variables.
- Customer feedback mechanisms—whether the automated system may generate complaints and what data should be captured in the new or existing complaints management system for analysis.
- Responsibility for monitoring and evaluation and taking action on learnings from the data.

A number of variables could be considered for monitoring and review, from business outcomes, to system statistics and client outcomes. Other important data will include budget and spending patterns, user and/or client numbers and feedback, and the ongoing monitoring and management of risks. Agencies should also be aware that program and policy areas of the agency may consider automated system data useful with regard to policy refinement.

Feedback and the incorporation of monitoring data will form an important picture of the success of an automated system project, in addition to creating a valuable source of information for the review, improvement and/or expansion of a system into the future.

Appendix A: Better practice checklist

The following checklist summarises items that should be addressed when considering the implementation or update of an automated system for administrative decision-making. A basic summary of the checklist can be found in the introduction to this Guide.

The checklist has been developed to assist agencies to assess the objective of an automated system at the point of development or redevelopment, and to ensure that agencies who automate decision-making are aware of their administrative and privacy law obligations when automated systems are used to administer government programs.

The checklist points are intended to be a guide for officers engaged in the design and/or implementation of automated systems, particularly policy owners, business analysts, system developers and administrative decision-makers.

The items in the checklists are not mandatory and are not intended to be comprehensive. Rather, they highlight key issues for agencies in relation to automated systems projects.

The checklist is iterative and feedback on how it can be improved is welcome.

●●●

Detailed checklist

Is an automated system suitable?

Have you ensured that the automated system does not, at any part of a process:

□ Contravene administrative law requirements of legality, fairness, rationality and transparency?

□ Contravene privacy, data security or other legal requirements (including human rights obligations)?

□ Compromise accuracy in decision-making?

□ Have a significant detrimental and irreversible impact on individuals and communities?

□ Significantly undermines public confidence in government administration?

Administrative law

□ Do the administrative decisions you propose to include in the automated system require the exercise of discretion or judgement by the assessing officer? If so, how does the system address the discretionary process?

□ Have you designed the system so that the decision-maker is not fettered in the exercise of any discretion or judgement they may have?

□ Has the automated system appropriately modelled parts of the administrative decision-making involving discretion and judgement?

□ Have all decision points in the automated system that involve the exercise of discretion or judgement been clearly identified as requiring human input, in the form of either a consideration of the facts or a review of a decision already made?

□ Are the business rules relating to discretion or judgement (and any research linked to such rules) contained in the automated system open to internal and external review?

□ Is notice provided to an affected individual before a decision is made?

Privacy

□ Is the automated system designed to collect only the minimum amount of personal information necessary to meet a clearly defined and articulated purpose?

□ Can the collection of personal information (that could identify an individual) be avoided or minimised, while still delivering a useful self-assessment tool?

□ Do self-assessment tools make it clear whether it is mandatory or optional for the individual to disclose some or all of the requested personal information?

□ Do self-assessment tools make clear whether information is being stored and/or retained for further use? Is the APP5 Notice within your automated system 'fit for purpose'?

□ Are there business processes to ensure that any release of information (outside of the purpose of collection, and for which an APP5 notice has been given) has been properly considered against the Privacy Act?

□ Are data-matching programs associated with use of the automated system properly authorised?

□ Is there legal authority to use existing data (previously collected for another purpose) for a new or secondary purpose?

Detailed checklist

- □ Does the automated system design enable notes of disclosure decisions (and reasons) to be appended to the record? Are appropriate security procedures in place to ensure the security of personal information?
- □ Have appropriate strategies been employed to manage the risk that outdated or unreliable data is used to make an automated decision?
- □ Does the automated system enable individuals to have access to the personal information collected (for example, via the generation of a personal information report where requested by an individual)?
- □ Do the business processes associated with use of the automated system have clear information access and complaint pathways?
- □ Is a privacy impact assessment required?

Governance and design

- □ Does the automated system project have appropriate formal governance arrangements?
- □ Is the scope of the automated system clear, and clearly reflected in project documentation?
- □ Have the relevant areas of legislation, policy or procedure been identified during the scoping phase? Have you considered the change management ramifications of the project?
- □ Have you developed a stakeholder and communications strategy to address the management of changed work practices for officers?
- □ Does the project plan involve consultation and input from the appropriate business and/or program areas? Have the relevant program areas/end users been consulted during the testing phase of the system?
- □ Do the project governance arrangements unambiguously assign policy ownership?
- □ Do the governance arrangements provide an appropriate role for the policy owner in the design, development, implementation and maintenance phases of the system?
- □ Do the project governance arrangements unambiguously assign project ownership?

The importance of multi-disciplinary teams

- □ Does the design team include officers with technical, legal, policy and service delivery experience?
- □ Have you consulted with the appropriate architecture, data and information management professionals within your agency environment?
- □ Where required, is the data mapping of terms and definitions relevant to the decision-making process interoperable with other agency IT systems?
- □ Will the automated system be required to process backdated administrative decisions?
- □ Does the design of the automated system allow for maintenance and execution of different versions of the business rules if required?
- □ If the underlying business rules of the automated system change, will the system be required to process changes to multiple decisions or records held within the system?
- □ Does the technical design of the automated system allow for the timely and efficient processing of changes to multiple decisions or records if required?

Detailed checklist

Verification with stakeholders

- □ Do the project governance arrangements provide for, and link with, a verification strategy and quality assurance process?
- □ Does the agency have appropriate verification processes, including visual verification of the underlying business rules as well as 'known outcome' scenario testing?
- □ Does the policy owner lead the 'known outcome' scenario-based testing process?
- □ Are the underlying business rules contained within the automated system accessible and readily understood by non-IT professionals?
- □ Does the verification strategy include a 'gap analysis' to assess whether the system design is appropriate to user needs, and is it being used as designed and intended?
- □ Does the verification strategy incorporate a review of user training to ensure the policy intention is communicated effectively and rapidly, and applied consistently?
- □ Does the verification strategy allow for external scrutiny by, and seek input from, external stakeholders?

Application of Digital Service Standards

- □ Have you ensured the Digital Service Standards are part of the system design?
- □ Have you considered deployment of the automated system through multiple service delivery channels (such as online, for self-assessment or via external agency systems)?
- □ Have you identified potential user groups for the automated system?
- □ Have you considered the impact of the automated system on your agency's channel management and service delivery strategies?
- □ Have you considered the access and equity issues that may arise, particularly if the automated system is to be deployed online or as a self-assessment tool?

Modelling and approval of business rules

- □ Do all members of the system design team share an understanding of the primacy of the law and is this understanding reinforced at all levels and stages of the automated system project?
- □ Are the business rules authorised by the law and verified as such by the policy owner?
- □ Where the automated system makes decisions, is this authorised by the relevant law, policy or procedure? Do the business rules mimic the structure and detail of the source legislation, policy or procedures?
- □ Have the business rules been referenced or linked to the source material (i.e. the specific part of the legislation, policy or procedures)?
- □ Where the automated system makes a decision, is this authorised by the relevant legislation?
- □ Have decisions about business rule definition relating to administrative decision-making discretion been adequately recorded?
- □ Have the business rules been reviewed (for example, by the policy owner) to ensure they accurately and comprehensively represent the relevant law, policy or procedure?

Detailed checklist

- □ Does the business rules review process examine discretion points to ensure they are not narrowly modelled or fettered?
- □ Do the project governance arrangements provide for settling anomalies and inconsistencies in legislation, policy or procedure?
- □ Have all areas of legislative or policy complexity and ambiguity been appropriately resolved?
- □ Has the automated system appropriately modelled parts of the administrative decision-making process involving the exercise of discretion and judgement?
- □ Does the automated system mandate the collation of the decision-maker's deliberations or reasoning on matters of discretion or judgement?
- □ Does the automated system provide links to relevant research and decision-support materials for each question or decision point contained in the system?

Maintenance

- □ Has adequate funding been secured for ongoing maintenance and upgrades to the system?
- □ Have clear business owner/s been identified as responsible for the ongoing maintenance and/or change requirements of the system?
- □ Do the project and quality assurance processes support the rapid approval and update of commentary within the system?
- □ Have testing processes been undertaken prior to and following implementation of the system? Are testing processes in place to verify modifications to the system or its business rules?
- □ Are strategies in place to ensure that the automated system's design and modifications history is documented?
- □ Are business continuity arrangements in place?
- □ Do business continuity management arrangements address the event of system unavailability or malfunctioning? Are officers able to make manual decisions if necessary?

Quality assurance

- □ Where automated systems interface with other agency IT systems, have you ensured that the accuracy of the legislative or policy rules within the automated system are not compromised (for technical efficiencies or otherwise)?
- □ Where automated systems interface with other agency IT systems, what measures have been taken to ensure systems interoperability and ease of update for the total solution?
- □ Have measures been undertaken to protect the integrity and quality of data held within the automated system?
- □ Do the governance arrangements and quality assurance processes support the rapid approval and update of commentary and user-support materials within the automated system?
- □ Is there a process in place to diagnose quality assurance problems, and to document how quality issues were resolved during the design process?

Detailed checklist

User training

□ Does the project plan include a training program for users of the system?

□ Have you established which of the following components the training program will include: business rules, legislation, use of the system, the wider business context and broader administrative decision-making skills?

□ Have officers in new or changed roles been appropriately trained for their new roles?

□ Has an ongoing training program for the users of a system been developed, including ongoing training updates for system enhancements?

Implementation

□ Have poorly designed and/or redundant business processes been re-engineered and/or retired?

□ Have you identified new business processes brought about by the automated system, such as mapping new business interactions, roles and responsibilities?

□ Has adequate consultation and stakeholder management been undertaken to address the change to new business processes?

□ Have you identified the likely impacts that implementation of the automated system will have on the usefulness and currency of older information technology infrastructure and systems?

Transparency and accountability

□ Is there any information about the automated system publicly available?

□ Are appropriate strategies in place to ensure that the business rules contained in the automated system are verified?

□ Are the business rules contained within the system in a form that can be readily understood by non-IT professionals?

□ Does the automated system have the capacity to automatically generate a comprehensive audit trail of the administrative decision-making path?

□ Are all the key decision points identifiable in the audit trail?

□ Are all the key decision points within the automated system's logic linked to the relevant legislation, policy or procedure?

□ Are all decisions recorded and accessible by the system's user, a reviewer or an auditor?

□ Is the audit trail secure from tampering (to provide protection and data integrity)?

□ Does the audit trail include a comprehensive and understandable modification history including:

- who created the document (with time and date recorded)?
- who has modified the document (with time and date)?
- a record of what was modified?
- for privacy and commercial-in-confidence matters, who has viewed the document (with time and date)?
- who made the final decision (with time and date)?

Detailed checklist

□ Does the audit trail start by identifying the authority or delegated authority identified in legislation? Does the audit trail show who an authorised decision-maker is?

□ Are all the decision points identifiable in the audit trail?

□ Can the audit trail generated by the automated system be easily integrated into a notification of the decision (including a statement of reasons or other notification) where required?

□ Are there review options for customers who dispute decisions?

□ Have you established a monitoring and review cycle for the automated system, including agreement on the information and data to be collected?

□ Have you considered collecting data that might be useful for policy and/or program refinement? If so, have you consulted the policy areas of the agency in relation to this issue?

□ Have you established appropriate user/client feedback mechanisms?

□ Have you clarified who has responsibility for the incorporation of learnings, monitoring and review?

□ Does the automated system's audit trail clearly set out decision points involving discretion or judgement?

□ Can the decision-maker's reasoning or deliberations (which are collected by the automated system where discretion or judgement is involved) be incorporated into a statement of reasons or other notification, where required?

□ Will the design of the audit trail assist with efficiently monitoring recommendations, decisions and processes? Does the audit trail feature in the agency's design for automated systems?

□ Will the audit trail's design meet the agency's business requirements, internal controls, transparency and accountability criteria, and audit requirements?

□ Have you designed the audit trail to include clearly identifiable links to authorised delegations (at every stage of the process)?

□ Will the audit trail's design provide for archiving and continuity of access?

□ Have you considered how change control processes will be reflected in the audit trail to:

- record modifications to the system's operation or performance?
- reflect changes to the legislation that underpins the operation of the system?

Appendix B:
Further reading and use cases

Administrative Review Council

Automated Assistance in Administrative Decision-making, Report No 46 (2004)

https://www.arc.ag.gov.au/Documents/AAADMreportPDF.pdf

Commonwealth Ombudsman

Centrelink's Automated Debt Raising and Recovery System—Implementation Report (2019)

https://www.ombudsman.gov.au/__data/assets/pdf_file/0025/98314/April-2019-Centrelinks-Automated-Debt-Raising-and-Recovery-System.pdf

Lessons learnt about digital transformation and public administration: Centrelink's online compliance intervention (2018)

https://www.ombudsman.gov.au/__data/assets/pdf_file/0024/48813/AIAL-OCI-Speech-and-Paper.pdf

Centrelink's Automated Debt Raising and Recovery System (2017)

https://www.ombudsman.gov.au/__data/assets/pdf_file/0022/43528/Report-Centrelinks-automated-debt-raising-and-recovery-system-April-2017.pdf

Digital Transformation Agency

Digital Service Standard

https://www.dta.gov.au/help-and-advice/about-digital-service-standard

European Union

General Data Protection Regulation
OJ L 119/1, art 22 (2016)

https://gdpr-info.eu/art-22-gdpr/

Federal Court of Australia

Justice Melissa Perry

iDecide: Digital Pathways to Decision (2019)

https://www.fedcourt.gov.au/digital-law-library/judges-speeches/justice-perry/perry-j-20190321

Government of Canada

Directive on Automated Decision-Making

https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32592

NSW Government Policy Lab

Emerging Technology Guide: Artificial Intelligence

https://www.digital.nsw.gov.au/digital-transformation/the-policy-lab

Appendix B: Further reading and use cases

NSW Ombudsman

Good conduct and administrative practice

https://www.ombo.nsw.gov.au/news-and-publications/publications/guidelines/state-and-local-government/good-conduct-and-administrative-practice

Office of the Australian Information Commissioner

Australian Privacy Principles Guidelines

https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/

Guide to Data Analytics and the Australian Privacy Principles

https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-data-analytics-and-the-australian-privacy-principles/

Guide to undertaking privacy impact assessments

https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-undertaking-privacy-impact-assessments/

Organisation for Economic Co-operation and Development

Recommendation of the Council on Artificial Intelligence OECD/Legal/0449 (2019)

https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449#_ga=2.201771153.1806885565.1559533436-1967103450.1558928769