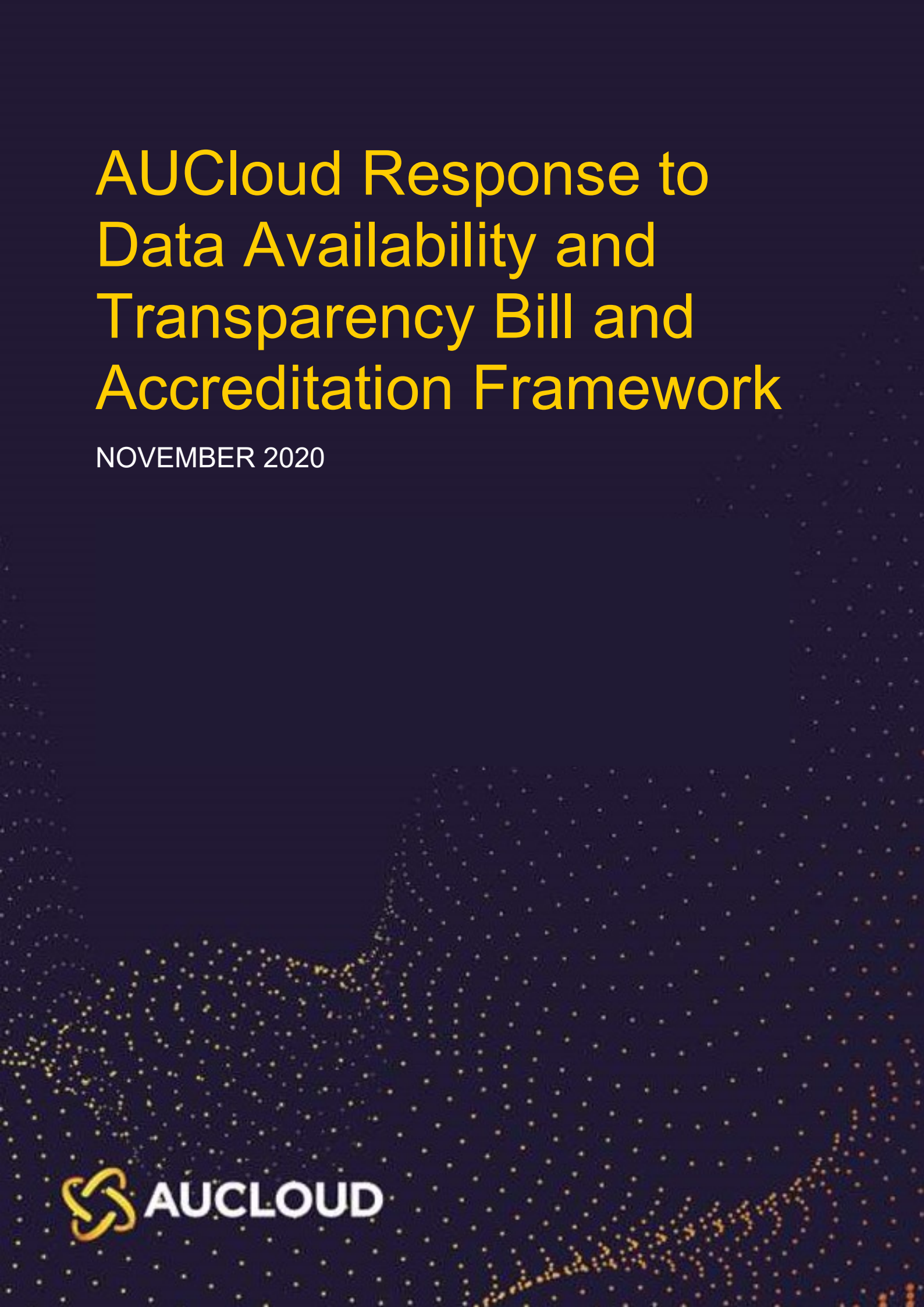
AUCloud Response to Data Availability and Transparency Bill and Accreditation Framework

NOVEMBER 2020



Disclaimer

The information in this Proposal is the confidential information of Sovereign Cloud Australia Pty Ltd ("AUCloud"). Such information must confidential at all times and used solely to consider the Proposal put forth by AUCloud. You agree to take such measures to prevent the disclosure of the information as you would to prevent the disclosure of your own proprietary information, but in all cases, shall use at least reasonable care.

You do not acquire any rights in the information. All AUCloud trademarks and logos belong to Sovereign Cloud Australia Pty Ltd. Other trademarks and logos belong to their respective owners and are used for informational purposes only.

The contents of this document constitute valuable proprietary and confidential property of AUCloud and are provided subject to specific obligations of confidentiality set forth in one or more binding legal agreements. Any use of this material is limited strictly to the uses specifically authorised in the applicable license agreement(s) pursuant to which such material has been furnished. In the event there are no applicable license agreement(s) governing the use of this material, please be advised that any use, dissemination, distribution, copying or disclosure of all or any part of this material not specifically authorised in writing by AUCloud in advance is strictly prohibited.

This is not a legally binding document and is submitted for information purposes only. Due to the forward-looking nature of this document, AUCloud's response may include information about solutions or products that may be in the planning stage of development or that may represent custom features or product enhancements. Feature and functionality cited in this document that is not publicly available or generally available today is discussed within the context of the strategic evolution of the proposed products. AUCloud is under no obligation to provide such future functionality.

Table of Contents

Introduction **3**

Response to the Data Availability and Transparency Bill and Accreditation Framework ... **4**

Proposed Framework 4

Accreditation Criteria 5

Accreditation Process 7

Other Matters 7

Consent to Data Sharing **8**

Introduction

Thank you for the opportunity to comment on the Data Availability and Transparency Bill and the Accreditation Framework discussion paper. We hope you find our comment useful in refining the Bill and Framework. Please do not hesitate to contact us on the submission contact details given if you would like to discuss any of our comments in more detail.

AUCloud is a sovereign cloud Infrastructure-as-a-Service (IaaS) provider, exclusively focused on meeting the needs of the Australian Government and Critical National Infrastructure (CNI) communities. This includes Federal, State and Local Governments and CNI organisations such as telecommunications, electricity, energy, financial services and similar utility providers.

Security is core to how we operate at AUCloud.

Independently IRAP assessed to the PROTECTED level controls of the Australian Signals Directorate (ASD) Information Security Manual (ISM). AUCloud provides two independent environments: an Official Data Community Environment (ODCE) and a PROTECTED Data Community Environment (PDCE) that meet or exceed these controls based upon the August 2020 version of the ISM.

In addition, AUCloud's IaaS offerings and supporting business processes have also been certified against the International Standard for Information Security (ISO/IEC 27001).

AUCloud solutions enable customers to benefit from sovereign data protection with the scale, automation, elasticity and lower costs typically associated with global cloud offerings.

As a sovereign IaaS provider, AUCloud is owned, managed and operated in Australia. All services and data managed by AUCloud remain in Australia ALWAYS (including metadata, monitoring data and derived analytics data). All AUCloud services are monitored and operated in Australia by Australian citizens who have been security cleared to Australian Government standards.

AUCloud operates from two Data Centres: Sovereignty Zone 1 in Canberra and Sovereignty Zone 2 in Sydney, both designed to meet ASIO T4 standards for Zone 4 security.

Response to the Data Availability and Transparency Bill and Accreditation Framework

Proposed Framework

1. What is considered to be an appropriate level of Australian ownership for an organisation to be eligible for accreditation?

   The underlying rationale for assessing the level of Australian "ownership" is not entirely explained.

   There are recent examples within the assessment of security risks, where the level of foreign influence has been questioned. For example, the recently introduced Cloud Assessment and Authorisation Framework, highlights the extra judicial risks that can be introduced as a result of using a company that ultimately has foreign ownership whereby access to the underlying data is asserted by the nationality of the ultimate parent company.

   It has already been proven that, from a security perspective, foreign-owned entities are trusted to handle Australian citizens' data on behalf of the Australian Government – for example with companies such as Amazon Web Services and Microsoft Azure hosting Government data in their Clouds and acceptance on the (since retired) Certified Cloud Services List (CCSL)[i]. Therefore, we challenge whether this is an appropriate consideration for accreditation.

   In the Section 4.2 of the discussion paper, the Data Commissioner would have to assess the risk of foreign interference in an accreditation decision. Therefore, the Data Custodian may have to similarly assess whether there are datasets which are sensitive enough to preclude even part-foreign owned entities from hosting, handling, or interpreting them, but are at the same time not too sensitive to be shared.

   If Australian ownership does become a requirement for accreditation, proving and guaranteeing this will be a complex process; for example:

   - Ownership would typically be defined in terms of equity but owning a majority share of a business does not always guarantee control or voting rights. Conversely, company decisions can often be influenced by minority, activist shareholders. It would need to be much more deeply understood what the risks of part foreign ownership are.
   - Secondly, if ownership is essentially a proxy for assessing the foreign control of a company, then debt should also be considered as a metric given the precedence this can take in the event of financial distress
   - In addition to debt considerations, contractual conditions should be considered such as 'step-in rights' that can pass effective operational control under certain conditions

2. Should individuals acting on behalf of an Accredited Data Service Provider be accredited individually? If so, what might be appropriate arrangements?

   The Framework identifies individuals as ones that either belong to the entity or who are acting on behalf of an entity, such as contractors, who would be bound by the entity's controls and processes anyway.

   The Framework's proposal to *'verify an individual's identity, test their understanding of their responsibilities under the legislation and collect other information relevant to their ability to manage, use and protect data appropriately'* is burdensome given that the responsibility could be adequately taken by the accredited entities, and that it is much simpler and more useful to accredit at the organisational level. For example, with the EU GDPR regulation, the organisation is responsible for

data protection and by extension responsible for ensuring they have adequate safeguards and processes in place for their employees to work within.

3. Are there circumstances when it should be mandatory to use an Accredited Data Service Provider for a data sharing project?

   Yes

4. What would those circumstances be?

   It is important to understand the context of the data sharing; provided are three theoretical examples:

   1. *What volume of data is being shared?*

      Entities may request a significant volume of data of many types, often to perform exploratory data analysis such as finding broad trends and correlations before narrowing their focus to specific areas of enquiry.

      However, there is inherently increased risk with the aggregation of data – for example, an individual may have lax arrangements for the security of a dollar, but stringent ones for the security of $10,000 in savings. Similarly, the tax records of an individual are not a target, but the tax records of the nation are. This is applied in the *Protective Security Policy Framework*[ii], where a piece of data could be rated OFFICIAL, but the loss of a whole database worth of OFFICIAL data raises their aggregate classification to PROTECTED.

   2. *What is the entity trying to achieve with the data?*

      This has to do with the discussed *Data Capability*: if the entity requesting the data has not proven themselves capable of generating the required insight from the data, then it could be mandated by the Custodian that they only receive the output of the data analysis by an accredited data service provider.

   3. *What is the sensitivity of the data?*

      It has been proven that anonymised or pseudonymised data can be re-identified when combined with other datasets. Techniques such as randomly sampling a subset of a dataset are sometimes used to prevent re-identification but are often not enough to prevent this happening: data that is considered de-identified can may not meet anonymisation standards such as those in GDPR.iii

      Therefore, there may be cases with sensitive data that advanced data capabilities would be required to ensure that the sensitive data of individuals is adequately protected.

Accreditation Criteria

5. Are there elements of data capability that should be given more or less weight in the accreditation process, i.e. making elements mandatory or optional?

   Items such as Executive level support, adherence to privacy principles, data sharing reporting and incident reporting should all be mandatory components of an accreditation framework. However, much of this is already captured in other standards that would cover a wider breadth of information and data security principles.

   There is no strict definition of capability given in the Bill or the Discussion Paper, but paraphrasing the UK data capability strategy, *'Seizing the data opportunity'*[iv], capability can be broken down in the following categories:

   - Skilled workforce – this would have to be optional, with stricter requirements depending on the context of the data sharing. As discussed in our response to question 4, a data custodian

may mandate the appointment of a statistician to perform data analysis if they doubted the capability of the individuals to correctly analyse the dataset.

- Tools and infrastructure – for example, mandatory data security requirements.
- Data as an enabler – this would not be mandatory and may fall under the advocacy function of the Data Commissioner. This could be known as 'corporate knowledge', with individuals and entities improving their maturity in sharing data appropriately, ensuring that adequate consent for sharing and analysis is sought at the point of collection, and more.

6. What elements would be most useful to Data Custodians to support their decision-making process when considering sharing and access to data?

Governance

This is likely to vary greatly depending upon the type of request but at a high level an understanding of governance arrangements and reporting would be crucial as part of any decision-making process. In questions 12 and 14 we discuss the transparency and availability of information related to breaches and suspensions.

Support and Guidance

There is a lot of responsibility being placed on Data Custodians to make thorough assessments, but the benefits will be realised by another entity. This may result in Data Custodians being very risk averse with little or no data sharing occurring.

A useful case in point is the appointment of 'Caldicott Guardians' in UK hospitals following the Caldicott review: these individuals were tasked with safeguarding patient data and were guided by six principles[v]. An unintended consequence of their effort was that data sharing was often restricted too much which was not in the patient's interest[vi]. Caldicott's second review 15 years later added the seventh principle:

'the duty to share personal information can be as important as the duty to have regard for patient confidentiality'

Consideration of the risk and benefit of sharing data will help ensure that Data Custodians will not only meet their duty to secure data, but to meet their duty to share data too.

Assistive Frameworks

Data Custodians will also need to know how to make a trade-off between risk and potential benefit of data sharing – this is within the advocacy function of the Data Commissioner as defined in the Bill. This could take the form of prescriptive frameworks (similar to a traditional risk matrix) developed by the Data Commissioner, that all Custodians could assess requests against. There will be discretion and subjectivity, but we expect this would help Data Custodians across Government to make consistent and well-devised assessments.

7. Should the accreditation process recognise other frameworks, standards or processes that have assessed an element of data capability? If so what standards/processes might be appropriate to recognise?

Yes, we believe it should. Significant effort has been put into other frameworks over time and it would be beneficial to build on their learnings about unintended consequences and the maturity growth of these. The discussion paper rightly recognises that building accreditation on top of existing frameworks ensures that leading practice can be implemented more easily and effectively.

There is a significant body of accreditation around the security of data, for example certifications such as ISO 27001, IRAP (PSPF/ISM) and others should be considered as mandatory for organisations wishing to be accredited.

8. Are there any elements of data capability that should be captured in order to understand an accredited entity's ability to keep data safe?

   The elements captured in Section 3.2 of the discussion paper would be sufficient.

Accreditation Process

9. What is a reasonable period of time to assess an application?

   We feel that the process should take no longer 4-8 weeks if all the correct information is given by the entity applying for accreditation.

10. Are there further ways we can streamline the accreditation process?

    As identified in the discussion paper, leverage other accreditation frameworks as applicable to other organisations.

11. Do the timeframes to renew accreditation, every 5 years for Accredited Data Service Providers and every 3 years for Accredited Users, seem reasonable?

    The timeframes appear to be excessive based on other accreditation frameworks. We would recommend ADSP every 2 years and Users every year.

Other Matters

12. Is it appropriate to notify parties to Data Sharing Agreements of an accredited entity's suspension?

    Yes, absolutely: the entire process should be transparent for all users of the program. If an entity is suspended all parties should be notified of such action and the reasoning behind the decision. It is often thought that process brings probity, but in our experience, it is transparency that does. If information is transparently available, decisions can be scrutinised.

    We expect the suspension of an entity would be material to parties of Data Sharing Agreements; for example, they may have to investigate whether they are affected, or at risk of being affected by a similar failure that leads to a data breach.

13. Is there any information that must, or must not, be made publicly available through the registers of accredited entities?

    We don't believe so.

14. Is there any information that should be made available to Data Custodians through the registers of accredited entities?

    Important to Data Custodians will be understanding whether an organisation has previously had data breaches. It may be beneficial if this information can be communicated in some form, at least for a specified period of time depending on the seriousness of the breach.

    The data custodians are expected to make a decision as to whether an entity is allowed to receive data, so it makes sense that they not only have the full information about security and more but also whether that entity has failed in its obligations before.

    If the Data Commissioner is tracking accreditation and breaches, then the Data Commissioner should provide Custodians with analysis of how the failure occurred, which the Custodian can use as a basis for more thorough assessment of the suitability of the entity to undertake the specified analysis.

    For example, when AUCloud responds to RFIs and RFQs with Government, it is a standard question if we are currently, or have previously been involved in legal disputes with the Government. We consider this a normal part of procurement's due diligence.

15. Is charging a fee for accreditation, such as a renewal fee, reasonable?

    Charging fees for services such as accreditation is not uncommon, though we recommend that the fees are reflective of an administration charge and not a way of raising revenue for two reasons:

    1. Charging fees will add friction, however small, to the process, which is at odds with the goal of improving data sharing to benefit Government service provision; and,
    2. if fees are too high, they preclude smaller entities from participating, which limits the pool of entities not to those most qualified, but those with the most money to spend on compliance.

Consent to Data Sharing

A key concern is the approach to consent as mentioned in Section 16.1.b of the bill:

> *any sharing of the personal information of individuals is done with the consent of the individuals, unless it is unreasonable or impracticable to seek their consent*

If this consent principle is to be used, the Data Commissioner needs to ensure that very strong controls are in place to ensure that Custodians and requesting entities are thoroughly exploring ways of getting consent. The risk is that it could easily be concluded in a review that getting consent is impracticable, and summarily dismissing the requirement to get it.

Further, as mentioned in the Bill discussion paper, the consent standard is modelled on the *'Privacy Act 1988',* but this effectively pre-dates the internet and so any consideration for mass data collection on the scale we see today.

When data is collected on such a large scale, it is not only the individuals' given data that must be protected, but metadata or derived data which results from the aggregation.

We note that this principle was elevated to be included in the Bill, but we think guidance should be strengthened, possibly through the Ministerial Rules, to stipulate the extent to which a Custodian has to go before deciding that consent is impracticable.

[ii] Protective Security Policy Framework - https://www.protectivesecurity.gov.au/information/sensitive-classified-information/Pages/default.aspx

[iii] Rocher, L., Hendrickx, J.M. & de Montjoye, Y. Estimating the success of re-identifications in incomplete datasets using generative models. *Nat Commun* **10,** 3069 (2019). https://doi.org/10.1038/s41467-019-10933-3

[iv] Seizing the data opportunity - https://www.gov.uk/government/publications/uk-data-capability-strategy

[v] Caldicott Principles - https://app.croneri.co.uk/topics/caldicott-principles-and-patient-confidentiality/indepth

[vi] Tough penalities and better data control – Caldicott - https://www.digitalhealth.net/2016/07/tough-penalities-and-better-data-control-caldicott/