Law Council
OF AUSTRALIA

Data Availability and Transparency Bill 2020

and

Data Availability and Transparency (Consequential Amendments) Bill 2020

Senate Finance and Public Administration Legislation Committee

17 March 2021

Telephone +61 2 6246 3788 • *Fax* +61 2 6248 0639
Email mail@lawcouncil.asn.au
GPO Box 1989, Canberra ACT 2601, DX 5719 Canberra
19 Torrens St Braddon ACT 2612
Law Council of Australia Limited ABN 85 005 260 622
www.lawcouncil.asn.au

Table of Contents

About the Law Council of Australia

The Law Council of Australia exists to represent the legal profession at the national level, to speak on behalf of its Constituent Bodies on national issues, and to promote the administration of justice, access to justice and general improvement of the law.

The Law Council advises governments, courts and federal agencies on ways in which the law and the justice system can be improved for the benefit of the community. The Law Council also represents the Australian legal profession overseas, and maintains close relationships with legal professional bodies throughout the world.

The Law Council was established in 1933, and represents 16 Australian State and Territory law societies and bar associations and the Law Firms Australia, which are known collectively as the Council's Constituent Bodies. The Law Council's Constituent Bodies are:

- Australian Capital Territory Bar Association
- Australian Capital Territory Law Society
- Bar Association of Queensland Inc
- Law Institute of Victoria
- Law Society of New South Wales
- Law Society of South Australia
- Law Society of Tasmania
- Law Society Northern Territory
- Law Society of Western Australia
- New South Wales Bar Association
- Northern Territory Bar Association
- Queensland Law Society
- South Australian Bar Association
- Tasmanian Bar
- Law Firms Australia
- The Victorian Bar Inc
- Western Australian Bar Association

Through this representation, the Law Council effectively acts on behalf of more than 60,000 lawyers across Australia.

The Law Council is governed by a board of 23 Directors – one from each of the constituent bodies and six elected Executive members. The Directors meet quarterly to set objectives, policy and priorities for the Law Council. Between the meetings of Directors, policies and governance responsibility for the Law Council is exercised by the elected Executive members, led by the President who normally serves a 12 month term. The Council's six Executive members are nominated and elected by the board of Directors.

Members of the 2021 Executive as at 1 January 2021 are:

- Dr Jacoba Brasch QC, President
- Mr Tass Liveris, President-Elect
- Mr Ross Drinnan, Treasurer
- Mr Luke Murphy, Executive Member
- Mr Greg McIntyre SC, Executive Member
- Ms Caroline Counsel, Executive Member

The Chief Executive Officer of the Law Council is Mr Michael Tidball. The Secretariat serves the Law Council nationally and is based in Canberra.

Acknowledgement

The Law Council of Australia acknowledges the contributions of the following Constituent Bodies and Committees in the preparation of this submission:

- New South Wales Bar Association;
- Law Society of South Australia;
- Queensland Law Society;
- Privacy Law Committee of the Law Council's Business Law Section; and
- Privileges and Immunities Committee of the Law Council's Federal Litigation and Dispute Resolution Section.

Executive summary

1. The Law Council appreciates the opportunity to respond to the Senate Finance and Public Administration Legislation Committee (**Committee**) inquiry into the Data Availability and Transparency Bill 2020 (Cth) (**DAT Bill**) and the Data Availability and Transparency (Consequential Amendments) Bill 2020 (Cth) (**Consequential Amendments Bill**) (together, **the Bills**).

2. The Bills seek to establish a framework for public sector data custodians to, under the relevant authorisations, principles, purposes and agreements, share data with accredited users under limited circumstances. In doing so, the Bills establish and specify the functions of the National Data Commissioner (**Commissioner**), as well as the National Data Advisory Council (**NDAC**) as an advisory body to the Commissioner.

3. The Law Council is generally supportive of the Bills and recognises the importance of fostering and facilitating government data sharing arrangements and the need for the continued development and improvement of robust policies to govern these arrangements.

4. However, the Law Council notes that the Parliamentary Joint Committee on Human Rights (**Joint Committee**) in considering the Statement of Compatibility with Human Rights, contained within the Explanatory Memorandum to the DAT Bill (**EM**), determined that 'further information is required in order to assess whether the stated objectives constitute a legitimate objective for the purposes of international human rights law'.[1]

5. While acknowledging the overarching public policy objectives of the Bills, with the questions that remain, Law Council shares the reservations of the Joint Committee as well as those matters raised by the Senate Standing Committee for the Scrutiny of Bills (**Scrutiny Committee**) about the potential risks associated with the scheme in practice.

6. Noting the potential risks of an improperly established data sharing scheme, the Law Council makes several recommendations aimed at improving the framework envisaged by the Bills, including that:

    (a) the Australian Government must ensure that sufficient funding is provided to the Commissioner to ensure that it is properly resourced to carry out its role;

    (b) amendment should be made to the DAT Bill to include minimum thresholds of training or experience for 'other persons' assisting the Commissioner in the exercise of their monitoring and investigation powers;

    (c) clause 105 of the DAT Bill should be removed as the proposed abrogation of legal professional privilege (**LPP**) is not sufficiently justified. In the alternative, consideration should be given to:

        (i) enabling an independent third-party, such as a court, to consider requests made by the Commissioner to resolve contested LPP claims on an expedited basis;

[1] Parliamentary Joint Committee on Human Rights, Parliament of Australia, *Human rights scrutiny report* (Report 2 of 2021, 24 February 2021) 18.

(ii) inclusion of a specific provision, similar to sections 79 and 95 of the *Law Enforcement Integrity Commission Act 2006* (Cth) (**LEIC Act**), enabling a lawyer to decline to comply with a notice to produce documents or provide information on the basis it is subject to LPP (which vests in their client) but requires the provision of the name and contact details of the client;

(iii) inclusion of a requirement that the Commissioner may only compel legally privileged information if satisfied, on reasonable grounds, that the compulsion is reasonably necessary and proportionate to the matter under investigation;

(iv) including explicit limitations in clause 108 the DAT Bill regarding the ability of the Commissioner to share information that is subject to LPP, or a claim of LPP; and

(v) amending clause 105 to provide that, if the Commissioner compels the production of legally privileged information, they are under a duty to ensure that it is held securely, protected from unauthorised access and disclosure and is securely destroyed or returned when no longer necessary for the investigation;

(d) amendment should be made to the DAT Bill to include an explicit requirement that, where possible, the sharing of data is done in a way that does not allow an individual to be identified and that de-identification should be the default or *prima facie* position prior to any sharing. Beyond the DAT Bill, consideration should also be given to expanding the definition of biometric data under the *Privacy Act 1988* (Cth) (**Privacy Act**) to include *all* biometric data not only the biometric information that is to be used for the purpose of 'automated biometric verification or biometric identification' or 'biometric templates' as is currently specified;

(e) the DAT Bill should be amended to provide that where privacy interests that involve biometric data may be affected by the data sharing scheme, all sharing of such data must be based on prior express consent;

(f) subclause 127(4) of the DAT Bill should be removed and a requirement should be inserted that the Guidelines to be made by the Commissioner are a legislative instrument and therefore subject to Parliamentary scrutiny and potential disallowance.

(g) further guidance is needed in relation to the scope of practical application of the 'unreasonable or impracticable' exception as it applies to securing consent, noting that this should be a high threshold to obtain and that many of the data sets collected are collected based on existing legal requirements or notices (not consents);

(h) Part 5.2 of the DAT Bill should be amended to provide greater detail in regard to the procedures, requirements and matters relating to the accreditation of entities for the purpose of the data sharing scheme; and

(i) merits review should be available to individuals and their representatives (as individual or representative complaints) whose privacy interests may be affected by the data sharing scheme.

Overview of the DAT Bill

7. The EM provides that the purpose of the DAT Bill is to:

> *Promote better availability and use of government data, empower the government to deliver effective policies and services, and support research and development.*[2]

8. To facilitate this purpose, the DAT Bill creates a new pathway for the Government to share public sector data by authorising a 'Data Custodian' (defined in the DAT Bill as Commonwealth bodies that 'control' public sector data and have 'the right to deal with that data')[3] to share data with an accredited user. The shared data can be provided directly to the accredited user or the sharing can be facilitated using an 'accredited data service provider' (**ADSP**).[4] The DAT Bill does not require data sharing, nor does it propose an open release of public sector data to the public. Instead, the sharing is intended to be a controlled and monitored communication of information to approved users.

9. Under the DAT Bill, Data Custodians would be authorised to share data with an accredited user, either directly or through an ADSP, if:

- sharing is for a permitted 'data sharing purpose' (including government service delivery, informing government policy and programs, or research and development);
- the five data sharing principles have been applied to manage the risks of sharing; and
- the terms of the arrangement were recorded in a data sharing agreement.[5]

10. Data scheme entities would be subject to data breach responsibilities, including an obligation to take steps to mitigate a data breach and a requirement to notify specified persons of a data breach.[6] Further, unauthorised data sharing would be subject to a civil penalty or up to two years' imprisonment where a person was reckless with respect to the circumstance that the sharing was not authorised.[7]

11. The DAT Bill would also establish an independent regulator, the Commissioner, whose role is to provide advice and advocacy, as well as oversee, investigate and enforce compliance. The DAT Bill also seeks to creates the NDAC to assist the Commissioner in their work.

Proposed oversight mechanisms

General principles

12. The Law Council acknowledges the importance of fostering and facilitating data sharing arrangements and the need for the continued development and improvement of robust policies to govern these arrangements. One of the arguments put forward for the Bills is that, currently, more than 500 secrecy provisions exist which can make sharing information very difficult, even when it is

[2] Explanatory Memorandum, Data Availability and Transparency Bill 2020 (Cth) 4.
[3] Data Availability and Transparency Bill 2020 (Cth) cl 11(2) ('DAT Bill').
[4] The accreditation framework is set out in pt 5.2 of the DAT Bill.
[5] DAT Bill cl 13(1).
[6] The data breach responsibilities are set out in pt 3.3 of the DAT Bill.
[7] DAT Bill cl 14.

appropriate to do so.[8] Addressing some of the inconsistencies between existing processes and protections may benefit the community, provided that privacy and security continues to be robustly protected.

13. The Law Council supports the removal of unnecessary barriers to government data sharing and the development of a single, unified approach to data sharing to improve the fragmented and often unclear approach that currently exists.[9] However, the Law Council also affirms the need for considered, robust and properly resourced oversight mechanisms and safeguards with regard to data sharing in order to uphold the rule of law, protect privacy and human rights, and to ensure that data is shared in a responsible way.

14. The Law Council acknowledges the oversight mechanisms embedded in the DAT Bill, including the creation of the Commissioner and the NDAC, as well as mandatory consideration of the following five data principles:

- project principle: data is shared for an appropriate project/program that includes consideration of the public interest, ethics, and privacy;
- people principle: data is made available only to appropriate persons who have the right training and skills;
- setting principle: data is shared in an appropriately controlled environment;
- data principle: appropriate protections are applied to the data – including data minimisation principles; and
- outputs principle: outputs are as agreed, and appropriate for future use.[10]

15. The use of 'appropriate' in the above principles requires a careful review on a case-by-case basis of novel (in the sense of previously unapproved) data sharing principles. Whether something is appropriate is a value-laden judgment which might be subject to review, and even retraction, in the event that further information comes to light with technological advances – 'data minimisation' consideration is but one example where advances in technology and handling practices might give reason for a re-assessment.

16. The proposed oversight mechanism provisions provide important safeguards to ensure that data sharing is carried out responsibly, ethically and ultimately protects public sector data and individual information, while balancing a need for efficiency which is carried out through data sharing agreements. These oversights also promote public confidence that the sharing of data will be done responsibly, because if an unauthorised sharing of data takes place, appropriate investigations and possible consequences will flow.

17. The Law Council supports these mechanisms and maintains that these protections should be actively reviewed and upgraded as required on an ongoing basis.

18. As an additional transparency mechanism, clause 130 of the DAT Bill requires the Commissioner to publish a public register of data sharing agreements and accredited entities. This aims to promote further transparency, as all sharing agreements are subject to public scrutiny. The Law Council supports the creation of this register and recognises this as an important safeguard mechanism.

---

[8] Office of the National Data Commissioner, Australian Government, *New Legislation* (Web Page) <https://www.datacommissioner.gov.au/data-sharing/legislation>.
[9] Law Council of Australia, Submission to Office of the National Data Commissioner, *Data Sharing and Release Legislative Reforms Discussion Paper* (22 October 2019) 1-2.
[10] DAT Bill cl 16.

19. Public scrutiny depends upon the disclosure of all information relating to the data sharing agreements including any commercial aspects of those agreements. It would defeat the purpose of that transparency if the parties to a data sharing approval might carve-out any part of the agreement having regard to commercial considerations.

20. Overall, the Law Council appreciates the delicate balance that must be struck between collecting and sharing data, and the right to privacy and appropriate safeguards. The Law Council considers that:

> *constraints on data sharing that are reliable, consistently implemented and verifiable… are necessary to ensure data sharing between government agencies is appropriately justified, controlled and transparent … regulatory settings must ensure data sharing outputs between government agencies are appropriately evaluated and managed, so that when those outputs are used to create outcomes that affect individual citizens (whether or not identified or identifiable), or targeted cohorts of citizens that are inferred through data analysis to share like characteristics, these outcomes are demonstrably fair, equitable, accountable and transparent.*[11]

21. It is important that the enactment of the Bills and the operation of the Commissioner and the NDAC are subject to appropriate regulations and active, ongoing oversight.

National Data Commissioner and National Data Advisor Council

Resourcing

22. The Commissioner will serve as the regulator for the data sharing scheme, provide advice and guidance about the scheme and be responsible for promoting understanding and acceptance of:

- the benefits of, and best practice in, sharing and releasing public sector data; and
- safe data handling practices.[12]

23. The Law Council supports the establishment of the role of the Commissioner (assisted by the NDAC) as a critical oversight and regulatory mechanism in the operation of the data sharing scheme. The Law Council submits that the Bill must be accompanied by sufficient funding to ensure the Commissioner is properly resourced to effectively carry out its role.

Recommendation:

- **The Australian Government must ensure that sufficient funding is provided to the National Data Commissioner to ensure that it is properly resourced to carry out its role.**

[11] Law Council of Australia, Submission to Office of the National Data Commissioner, *Data Sharing and Release Legislative Reforms Discussion Paper* (22 October 2019) 2.
[12] Ibid cl 39, 42.

‘Other persons’

24. Subclauses 109(4) and 110(3) of the DAT Bill would allow the Commissioner (as an authorised person) to receive assistance from ‘other persons’ in the exercise of their monitoring and investigation powers. The Law Council notes the concern of the Scrutiny Committee that these provisions provide ‘no requirement … that the other person has appropriate training or experience’.[13] In response to the concerns of the Scrutiny Committee, the Minister advised that:

> *The standard suite of [Regulatory Powers (Standard Provisions) Act 2014] provisions is an accepted baseline of powers required for an effective monitoring, investigation or enforcement regulatory regime, while providing adequate safeguards and protecting important common law privileges … The Bill adopts this standard approach to the exercise of regulatory powers to promote an efficient, flexible and accountable approach to regulation.*
>
> *The Explanatory Memorandum for clauses 109 and 110 refers to the staffing provisions in the Bill [Explanatory Memorandum, Data Availability and Transparency Bill 2020, paras 555 and 560] The Bill’s staffing provisions ensure that ‘other persons’ at the Commissioner’s disposal will have the appropriate knowledge, training and expertise in the exercise and performance of investigatory powers and functions [see clauses 47-49 of the Bill]. APS employees made available to the Commissioner must have the skills, qualifications or experience necessary to assist the Commissioner, while contractors and consultants may be specifically engaged in order to assist with the performance or exercise of the Commissioner’s functions or powers.*
>
> *Subsections 23(2)-(4) of the RPA ensure monitoring and investigatory powers are exercised accountably. Persons assisting must act under the direction of the Commissioner as authorised person and any valid actions of the person assisting will be taken to be those of the Commissioner. As persons employed or engaged by an APS Department, assisting individuals will be further subject to standard accountability measures such as the APS Code of Conduct (for staff), Commonwealth Procurement Rules (for contractors), security clearances and other pre-employment screening procedures.*[14]

25. However, the Scrutiny Committee has maintained its concern that there is no apparent requirement on the face of the DAT Bill that the ‘other persons’ assisting an authorised person (the Commissioner) must be the staff, consultants or contractors to which clauses 47-49 of the DAT Bill refer.[15] On this basis the Scrutiny Committee reiterated its ‘consistent scrutiny view in relation to the exercise of coercive or investigatory powers that persons authorised to use such powers should have appropriate training and experience’.[16]

---

[13] Senate Standing Committee for the Scrutiny of Bills, Parliament of Australia, *Scrutiny Digest* (Digest No 3 of 2021) 23-6 (‘Scrutiny Committee Report’).
[14] Hon Stuart Robert MP, Minister for the National Disability Insurance Scheme, Minister for Government Services, *Response to the Senate Standing Committee for the Scrutiny of Bills - Scrutiny Digest 1 of 2021 Data Availability and Transparency Bill 2020* (2021) 9.
[15] Senate Standing Committee for the Scrutiny of Bills, Parliament of Australia, *Scrutiny Digest* (Digest No 3 of 2021) 25.
[16] Ibid 25-6.

26. The Law Council supports the view of the Scrutiny Committee and recommends that minimum thresholds of training or experience for other persons assisting the Commissioner in the exercise of their monitoring and investigation powers be included in the DAT Bill.

Recommendations:

- **Amendment should be made to the Data Availability and Transparency Bill 2020 (Cth) to include minimum thresholds of training or experience for 'other persons' assisting the Commissioner in the exercise of their monitoring and investigation powers.**

Legal Professional Privilege

Background

27. Clause 104 of the DAT Bill provides the Commissioner with a power to require information and documents if the Commissioner 'reasonably believes that a person has information or a document relevant to an investigation under section 101, or to any other of the Commissioner's regulatory functions set out in section 45'.

28. Clause 105 provides that LPP (also known as client legal privilege) is not a basis for refusing to provide information or documents sought by the Commissioner under clause 104. Clause 105 provides:

> *(1) A person is not excused from complying with a notice under section 104 on the ground that giving the information or producing the document would disclose a communication protected against disclosure by legal professional privilege.*
>
> *(2) However:*
>
> *(a) the information given or document produced; and*
>
> *(b) the giving of the information or production of the document;*
>
> *are not admissible in evidence against a person in any civil or criminal proceedings.*
>
> *(3) The fact that a person is not excused from complying with the notice on the ground mentioned in subsection (1) does not otherwise affect a claim of legal professional privilege that anyone may make in relation to that information or document.*

29. LPP is a fundamental and basic doctrine of the common law that protects confidential communications between a lawyer and client made for the dominant purpose of the lawyer providing legal advice or professional legal services or for use in current or anticipated litigation.

30. The rationale for LPP is to enhance the administration of justice and the proper conduct of cases by promoting the full and frank disclosure between the client and the legal practitioner, which allows people to obtain accurate and comprehensive advice about their legal situation. This has the effect of facilitating greater compliance with the law and more effective and efficient resolution of legal disputes.

As stated by Kirby J in *Esso Australia Resources v Commissioner of Taxation* discussing the purpose of privilege:

> *It arises out of 'a substantive general principle of the common law and not a mere rule of evidence'. Its objective is 'of great importance to the protection and preservation of the rights, dignity and freedom of the ordinary citizen under the law and to the administration of justice and law'. It defends the right to consult a lawyer and to have a completely candid exchange with him or her. It is in this sense alone that the facility is described as 'a bulwark against tyranny and oppression' which is 'not to be sacrificed even to promote the search for justice or truth in the individual case'.*[17]

31. As is recognised in the EM to the DAT Bill, '[l]egal professional privilege is an important right that ought to be abrogated only where there is strong justification'.[18] In this regard, it is proposed in the EM that:

> *Abrogation is justified here in order to serve higher public policy interests in the effective regulation and enforcement of the Bill, to ensure integrity of the data sharing scheme and protection of public sector data.*
>
> *In particular, the abrogation of legal professional privilege is necessary as data scheme entities are likely to obtain legal advice before entering into data sharing agreements that may be material to investigations under this clause. This information is likely to be central to the issues being considered by the Commissioner's investigations, but unlikely to be available from an alternate source. Abrogation of this privilege will allow the Commissioner to effectively hold data scheme entities to account for their handing of government information, an outcome in which there is a strong public interest.*
>
> *This approach is also informed by other regulators' experience, whose investigatory activities have been delayed or hampered by an inability to access relevant information, and the difficulty establishing the bounds of the privilege.*[19]

32. The existence of LPP reflects, to the extent to which is accorded, the paramountcy of the public interest in enhancing the administration of justice by facilitating the representation of clients by legal advisers. Public policy recognises that the law is a complex and complicated discipline and that if a client is unable to keep secret their communications, they will not be induced to seek proper legal advice nor be encouraged to make a full and frank disclosure of the relevant circumstances to their lawyer.

Proposed justification for the abrogation of LPP

33. In the Law Council's view, the justification as set out in the EM to the DAT Bill is insufficient to justify the proposed abrogation of LPP.

    (a) There are many enforcement authorities/agencies that would like to read the legal advice obtained by persons whom they wish to investigate (similar justifications could be made, for example, by the Australian Tax Office or

[17] (1999) 201 CLR 49, [111] (Kirby J).
[18] Explanatory Memorandum, Data Availability and Transparency Bill 2020 (Cth) [526].
[19] Ibid [526]-[528].

Australian Securities and Investments Commission (**ASIC**) with respect to their investigations). Notwithstanding the strong public interest in ensuring that Australian taxpayers do not avoid their tax obligations, and the strong public interest in ensuring that Australian Financial Services License holders operate honestly efficiently and fairly, and that directors and corporations meet their statutory obligations, abrogation arguments with respect to those agencies have been plainly rejected on public policy grounds previously. In circumstances where the legislature recognises the public interest in maintaining LPP is greater than the public interest in facilitating investigations by the ATO Commissioner, the DAT Bill is not justified in seeking to elevate the powers of the National Data Commissioner above others such as the ATO Commissioner.

(b) The fact that it is not possible to obtain a copy of that legal advice without statutory abrogation is insufficient justification for abrogation itself. There is a countervailing, weightier public policy justification for maintaining LPP. While there is a public policy interest that investigations and trials are able to be conducted on the footing that all relevant documentary evidence is available, LPP is so firmly entrenched in the law and policy, that revelatory investigations and the conduct of trials do not exorcise the privilege. No doubt prosecutors and litigants would enjoy access to privileged communications of the counterparties, but the law does not accept that the interests of an investigation or fair trial warrant the abrogation of LPP.

(c) Similarly, the fact that investigations might be delayed or even hampered by an inability to access legal advice obtained by the subject of the investigation is insufficient to justify abrogation. Both the Australian Federal Police and ASIC have in the past expressed frustration that their investigative processes have been slowed down through the making of privilege claims that have been viewed as obstructionist rather than (claiming) warranted legal rights. However, the response to that is to create mechanisms for the speedier determinations of any contested privilege claims. It does not (nor has it) justified the abrogation of such a fundamental legal right as LPP.

34. The Law Council does not consider the reference in the EM to the DAT Bill to other legislation conferring coercive information-gathering powers on other agencies to be an adequate justification for the proposal to abrogate LPP in this case.[20] The need for the override must always be justified in relation to the particular investigative agency. As it stands in relation to the DAT Bill, sufficient explanation has not been provided.

35. While the legislature has abrogated the privilege against self-incrimination in a number of instances (subject to immunity against the use of those answers in prosecutions), the abrogation of LPP is such a significant step that it is most uncommon. There is a very sound reason for this. The abrogation of LPP grossly undermines the ability of persons to obtain confidential legal advice about the subject matter in question.

36. If LPP was abrogated as proposed, it would preclude a person from obtaining legal advice about its responsibilities within the DAT regulatory regime, about the veracity of its conduct or the regulator's conduct or advice about the Commissioner's conduct, without the risk of that advice being exposed.

[20] Ibid [535]

37. The proposition that abrogation of LPP will allow the Commissioner to hold data scheme entities to account for the handling of government information is inconsistent with the fact that the Bill provides for the inadmissibility of that material in any civil or criminal proceedings.

Proposed restrictions on the abrogation of LPP

38. The Bill does include some restrictions on the abrogation of LPP.

    (a) Subclause 105(2) (extracted above), provides that information and documents given to the Commissioner pursuant to clauses 104 and 105(1), and the act of providing information or documents, are not admissible in evidence against a person in any civil or criminal proceedings.[21] The EM describes this as 'broad use immunity' as it protects all persons, not only the person who produced the materials or is entitled to claim the privilege.[22]

    (b) Subclause 105(2) (extracted above), states that production under compulsion 'does not otherwise affect a claim of legal professional privilege that anyone may make in relation to that information or document'. Presumably, this is intended to mean that compulsory production does not amount to a waiver of LPP by the person entitled to make that claim. This could be made more explicit.

39. The key point to note, however, is that the policy rationale for seeking abrogation of LPP is insufficient. In the circumstances, limitations placed on the use of abrogated information and documents is little consolation.

40. There exists a balancing act between the public interest that regulatory investigations be conducted efficiently and the interest in allowing lawyers to advise their clients appropriately knowing the protections of privilege remain intact. The Law Council opposes the abrogation of LPP as proposed by the DAT Bill, notwithstanding the proposed limitations in relation to how privileged information may be used.

Attorney-General's public interest certification regime (clause 106)

41. Clause 106 is also intended to provide some limitation on the power to require information and documents. Subclauses 106(2) and (3) specify that the Attorney-General may provide the Commissioner with a 'public interest certificate' which prevents the Commissioner from requiring information or documents if doing so would be contrary to the public interest (for example, because it would prejudice the conduct of an investigation or inquiry into crime or criminal activity that is currently being pursued or prejudice the fair trial of any person).

42. Reliance on the *ad hoc* exercise of executive discretion fails to provide meaningful protection to sensitive information, consistent with the requirements of the rule of law that the law should be clear and certain in advance of its application to particular circumstances.

43. The Law Council also generally opposes such certification regimes as they are contrary to the independence of the relevant oversight or investigatory bodies (in this case the Commissioner), by making their access to necessary information to perform their functions contingent on the discretion of a Minister (the Attorney-

[21] Ibid [530].
[22] Ibid.

General).[23] Access to information separate to the actions of the Minister is essential to the independent functioning of such bodies. Instead, the focus should be on resourcing and 'up-skilling' the relevant oversight or investigatory bodies to handle and protect classified or otherwise sensitive information.

44. The Law Council also notes in the context of a protection for information subject to LPP, the public interest-related grounds for issuing a certificate in subclause 106(3) do not squarely cover privileged information. Rather, it would be the subject-matter of the communication (for example, inter-governmental communications, or law enforcement investigations, or matters pertaining to national security or defence) that would give rise to the issuing of a certificate. The fact that any such information is also subject to LPP would be purely coincidental.

45. In the Law Council's view, clause 106 does not provide meaningful protection for legally privileged information, and moreover is problematic in its own right because it makes the Commissioner's access to information (and the availability of protection) dependent on the *ad hoc* exercise of discretion by the Attorney-General.

Law Council recommendations

46. However, it is important to note that there is nothing contained in the DAT Bill to prevent the derivative use of information or documents obtained pursuant to clauses 104 and 105(1). As is noted in the EM to the DAT Bill:

> *The immunity does not extend to derivative use, as that would exclude all evidence discovered in reliance on leads from the disclosure (in contrast to the use immunity that renders inadmissible only the evidence that was disclosed).*[24]

47. The Law Council strongly opposes the proposed blanket abrogation of LPP, particularly as it does not prevent derivative use, which fundamentally undermines any purported protections that the DAT Bill might seek to create. In reality, derivative use would mean that no meaningful protection exists.

48. In the Law Council's view, clause 105 should not proceed, unless and until adequate justification is provided, which addresses the specific need for the Commissioner's information-gathering powers to override LPP and excludes less-restrictive alternatives. The Parliament and wider public, particularly the national legal profession, should be given an adequate opportunity to scrutinise any justification provided before the Bill is debated.

49. As noted above, LPP exists to promote the public interest by ensuring frank discussion and candour between a legal practitioner and a client, thereby advancing the administration of justice and promoting compliance with the law. The Law Council is very concerned that the proposed abrogation of LPP may discourage people or organisations from obtaining legal advice which may have otherwise facilitated better compliance with the data sharing scheme. There is also the potential for adverse inferences being drawn about the legal practitioner's client for having sought legal advice from a practitioner. As noted by Deane J in *Baker v*

[23] The Law Council has raised similar concerns in relation to section 149 of the *Law Enforcement Integrity Commission Act 2006* (Cth) (which is proposed to be subsumed in the proposed Commonwealth Integrity Commission Act) amd subsection 9(3) of the *Ombudsman Act 1976* (Cth).
[24] Ibid.

Campbell, 'a person should be entitled to seek and obtain legal advice in the conduct of his affairs … without the apprehension of being thereby prejudiced'.[25]

50. Should clause 105 of the DAT Bill not be removed, the Law Council recommends that consideration be given to enabling an independent third-party, such as a court, to consider requests made by the Commissioner for information or documents that are otherwise protected against disclosure by LPP.[26] In the Law Council's view, this would assist in avoiding unnecessary delays in investigations while better ensuring that LPP is not unreasonably abrogated.

51. The Law Council is concerned by the possibility that a regulated entity's lawyer could be the target of coercive information-gathering powers, in respect of legal advice they have provided to the regulated entity, for the purpose of the Commissioner investigating that regulated entity. This differs significantly from the model under the LEIC Act. Sections 79 and 95 of the LEIC Act contain specific provisions enabling a lawyer to decline to comply with a notice to produce documents or provide information on the basis it is subject to LPP (which vests in their client) but they are required to provide ACLEI with the name and contact details of the client. Should clause 105 be maintained, the Law Council suggest that a provision similar to those in the LEIC Act be included to ensure that clause 105 does not compel a lawyer to betray their client's privilege, should the Commissioner attempt to serve the lawyer with a notice to produce information or documents under clause 104 and rely on the override in clause 105. In addition, inclusion of a requirement that the Commissioner may only compel legally privileged information if satisfied, on reasonable grounds, that the compulsion is reasonably necessary and proportionate to the matter under investigation.

52. The Law Council is also concerned that clause 108 confers a wholesale discretion on the Commissioner (or their staff) to disclose any information obtained in the course of the Commissioner performing their functions to a wide range of other agencies. This includes a number of listed agencies as well as any other agency or body prescribed in the rules (with no limitations or criteria governing the agencies that may be prescribed). There are no limitations on the disclosure of privileged information. While proposed s 105 will provide use immunity in both criminal and civil proceedings and purports to preserve claims to privilege in relation to any entity other than the Commissioner, the ability to disclose confidential lawyer-client communications about the subject-matter of an existing, imminent or potential enforcement matter (including criminal charge) and for the receiving enforcement agency to use that information derivatively, may effectively nullify the value and utility of that privilege.

53. Should clause 105 be maintained, explicit limitations should be included in the DAT Bill regarding the ability of the Commissioner to share information that is subject to LPP, or a claim of LPP.

[25] (1983) 153 CLR 52, [8].

[26] See, eg, *Royal Commissions Act 1902* (Cth) s 6AA: this section effectively operates as a defence to the offence of non-compliance with a notice to produce documents or provide information. It is available where a court has determined that the information is subject to LPP, or a claim has been made to a royal commissioner who may accept or reject the claim (on the basis of the law of LPP, not a public interest assessment on the grounds that the information is privileged but the public interest in disclosure is overriding). See also *Independent Broad-Based Anti-Corruption Commission Act 2011* (Vic) s 147. As can occur in the Victorian anticorruption body, the *Independent Broad-Based Anti-Corruption Commission Act 2011* (Vic) which provides for an application to be made pursuant to section 147 of the Act to the Supreme Court for a determination to be made in relation to any claim of privilege.

54. Consideration should also be given to amending clause 105 to provide that, if the Commissioner compels the production of legally privileged information, they are under a duty to ensure that it is held securely, protected from unauthorised access and disclosure and is securely destroyed or returned when no longer necessary for the investigation. Such a provision would provide clear benchmarks for consistent best practice, and for audit and oversight of compliance.

Recommendations:

- **In the absence of compelling explanation of the perceived need to compel privileged information, proposed section 105 should be omitted from the Bill.**
- **In the alternative, consideration should be given to:**
  - **enabling an independent third-party, such as a court, to consider requests made by the National Data Commissioner to resolve contested LPP claims on an expedited basis;**
  - **inclusion of a specific provision, similar to sections 79 and 95 of the *Law Enforcement Integrity Commission Act 2006* (Cth), enabling a lawyer to decline to comply with a notice to produce documents or provide information on the basis it is subject to LPP (which vests in their client) but requires the provision of the name and contact details of the client;**
  - **inclusion of a requirement that the Commissioner may only compel legally privileged information if satisfied, on reasonable grounds, that the compulsion is reasonably necessary and proportionate to the matter under investigation;**
  - **including explicit limitations in clause 108 the Data Availability and Transparency Bill 2020 (Cth) regarding the ability of the National Data Commissioner to share information that is subject to LPP, or a claim of LPP; and**
  - **amending clause 105 to provide that, if the National Data Commissioner compels the production of legally privileged information, they are under a duty to ensure that it is held securely, protected from unauthorised access and disclosure and is securely destroyed or returned when no longer necessary for the investigation.**

Self-incrimination privilege

55. Although the EM to the DAT Bill states that the Bill 'does not displace the common law privilege against self-incrimination', the Law Council notes the silence of the Bill in this regard.[27] Despite this silence, the Law Council notes that the contention in the EM is consistent with the principle of legality in statutory interpretation (under which self-incrimination privilege has been recognised as a fundamental right that requires clear words to abrogate it).[28]

56. In the Law Council's view, it is preferable for the Bill to expressly state that potential self-incrimination is a basis upon which a person may decline to comply with a notice under clause 104. There should also be an express preservation of 'penalty

[27] Explanatory Memorandum, Data Availability and Transparency Bill 2020 (Cth), [534].
[28] See, eg, *X7 v Australian Crime Commission* (2013) 248 CLR 92.

privilege' in relation to exposure to civil penalty as a result of compliance with a clause 104 notice. This would also provide the strongest and clearest possible assurance that self-incriminating information obtained under compulsion via an s 104 notice could not then be shared under proposed s 108 with law enforcement agencies for the purposes of investigations or enforcement proceedings.

Privacy considerations

57. When discussing data sharing arrangements, consideration must be given to any impact upon privacy, particularly when these arrangements involve not just intragovernmental sharing, but also third party and private sector entities. The Law Council notes that most personal information collected by government agencies is collected pursuant to legal requirements for a given purpose. The proposed data sharing arrangements will put large segments of such information to new uses and new disclosures which may not have been anticipated or contemplated at the time of collection. This of itself is a very privacy intrusive measure and requires careful consideration to ensure that newly created privacy risks are appropriately addressed or mitigated.

58. The Privacy Act protects and promotes the privacy of individuals and regulates how Australian government agencies handle personal information. The Law Council notes that the Privacy Act has been the subject of a number of reviews over the past 12 years, including a current review by the Attorney-General's Department.[29]

59. The Consequential Amendments Bill will amend the Privacy Act by including the Commissioner as an alternative complaint body.[30]

Human rights compatibility

60. The Law Council notes the comment by the Joint Committee that '[g]iven the breadth and depth of information which could be shared, and with a wide group of entities, the proposed measure engages and limits the right to privacy'.[31] The Joint Committee reported in February 2021 that:

> *the committee notes that the statement of compatibility does not, itself, set out what objectives are sought to be achieved by the [DAT Bill]. Accordingly, the committee considers that further information is required in order to assess whether the stated objectives constitute a legitimate objective for the purposes of international human rights law. Further, the committee notes that, while the statement of compatibility provides a list of safeguards with respect to the right to privacy, the extent to which the proposed scheme may limit the right to privacy is not clear.*
>
> *The committee has not yet formed a concluded view in relation to this matter. It considers further information is required to assess the human rights implications of this bill.*[32]

[29] Attorney-General's Department, Australian Government, *Review of the Privacy Act 1988* (Web Page, 2020) <https://www.ag.gov.au/integrity/consultations/review-privacy-act-1988>. See also Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice* (Report No 108, May 2008); Australian Law Reform Commission, *Serious Invasions of Privacy* (Report No 123, June 2014); Australian Competition and Consumer Commission, *Digital Platforms Inquiry* (Final Report, July 2019).
[30] Data Availability and Transparency (Consequential Amendments) Bill 2020 (Cth) cl 6-8.
[31] Joint Committee Report, 18.
[32] Ibid.

61. The Joint Committee considered that the extent to which the scheme may limit the right to privacy was not clear and has sought the Minister's advice with respect to a range of matters related to the right to privacy including:

> *(c) in what type of circumstances is it likely that data will be shared, or not shared, for a data sharing purpose (with examples provided as to what is, and is not, likely to be considered to be for 'the delivery of government services'; 'informing government policy and programs'; and 'research and development);*
>
> *(d) what considerations would be considered relevant (and irrelevant) in an assessment of the 'public interest' for the purpose of proposed subclause 16(2), and why does the [DAT Bill] not specifically reference the need to consider the right to privacy;*
>
> *(e) in what circumstances, and based on what factors, would it be considered unreasonable or impracticable (under proposed paragraph 16(2)(c)) to seek the consent of individuals whose personal information would be shared, and would the provision of any government service be contingent on the individual giving their consent to the proposed sharing of their data;*
>
> *…*
>
> *(i) in what circumstances does the bill provide, and is it intended that the rules will provide, that a data sharing agreement may allow the accredited user to provide shared output data to a third party, and what protections apply to protect personal privacy in such circumstances; and*
>
> *(j) why other, less rights restrictive alternatives would not be effective to achieve the intended objectives (such as amendments to individual pieces of legislation to invoke this data sharing scheme which take into account the specific data to be shared and the specific circumstances in which it is appropriate to share such data).*[33]

62. In the Law Council's view, further clarity around these issues is essential for both consumers and for government and non-government businesses who require access to Commonwealth data. This needed to address the existing requirements of the Privacy Act and to ensure that there is trust in the system and the personal information sought to be shared as part of the newly created framework.

63. The Joint Committee have also raised concerns with respect to the sharing of data for 'delivery of government services' and in particular, whether this would encompass withholding government services such as social security payments.[34] The Privacy Impact Assessment of the Draft DAT Bill has previously highlighted stakeholder concerns with respect to the need for a robust ethics framework around how automated decision making is treated to provide assurances against the use of data as a tool for discrimination.[35]

64. While the EM to the DAT Bill indicates that data scheme entities would need to comply with rules and data codes,[36] as noted by the Joint Committee, there is no

[33] Ibid 16-7.
[34] Ibid 9-10.
[35] Information Integrity Solutions for the Office of the National Data Commissioner, Australian Government, *Privacy Impact Assessment – Draft Data Availability and Transparency Bill 2020* (6 September 2020) 23.
[36] Explanatory Memorandum, Data Availability and Transparency Bill 2020 (Cth) 35.

guidance in the legislation as to their contents, clause 26 of the DAT Bill simply states that a data scheme entity must comply with them.[37]

65. Therefore, while acknowledging the overarching public policy objectives of the Bills, with the questions that remain, the Law Council shares the reservations of the Joint Committee about the potential risks associated with the scheme in practice and considers the Minister's response to the Joint Committee's queries to be critical.

Scope of the proposed scheme

66. It is noted that the operation of the proposed scheme is considered in light of the involvement of third parties. As an example, personal medical details may be able to be made available under the proposed regime to allow a third party to create an app or other form of product or service on behalf of the government. In these circumstances, the proposed regime would then rely on the data management agreement that is entered into to manage the data and, importantly, its use and security. Doing so leaves the effectiveness of the regime largely in the hands of the drafters of the agreements, which may seem rather open to abuse.

67. Noting this approach and the risks inherent in the proposed scheme Law Council draws the Committee's attention to several aspects of the DAT Bill in terms of its scope and potential application.

Type of data collected

68. The Law Council notes that the term 'public sector data' in the DAT Bill is broadly defined at clause 10 as 'data lawfully collected, created or held by or on behalf of a Commonwealth body'. This definition is wide and potentially encapsulates all types of data including data relating to health, finances and criminal history (biometric data is discussed in further detail below). The Law Council notes the sensitive and serious nature of this type of information and suggests that further consideration should be given to the ways in which public sector data could be shared, particularly relating to sensitive information, and subsequently infringe on an individual's privacy. Consideration should also be given to ensuring that data is appropriately de-identified, or where that is not possible, masked or minimised. This needs to be a matter of standard practice, done by 'design and by default', and form part of a legal requirement to do so.

69. The potential sharing of personal information requires particularly careful consideration. While the Law Council acknowledges the restrictions in the DAT Bill (such as ensuring that in order to share data, it must be for a permitted purpose), there is a risk that data sharing may still be inadvertently facilitated in circumstances where it should not be allowed.

70. Noting this risk, the Law Council submits that the DAT Bill should contain provisions requiring the de-identification of personal information prior to sharing the information. While it is recognised that anonymisation is limited in its capacity, some of the people submitting data to government agencies may be vulnerable and, potentially, less eager to engage if they knew their open data may be shared at will, whether under the auspices of a managed regime or not. If need be, these special circumstances can be addressed in appropriately worded exemptions.

[37] Joint Committee Report, 15.

71. On this point, the Law Council notes that the Scrutiny Committee has raised concern as to:

> *the appropriateness of the [DAT Bill] not including an explicit requirement that, where possible, the sharing of data is done in a way that does not allow an individual to be identified.*[38]

72. The Law Council shares this concern and agrees with the view of the Scrutiny Committee recommends that the DAT Bill be amended to include an explicit requirement that, where possible, the sharing of data is done in a way that does not allow an individual to be identified.

Recommendation:

- **Amendment should be made to the Data Availability and Transparency Bill 2020 (Cth) to include an explicit requirement that, where possible, the sharing of data is done in a way that does not allow an individual to be identified and that de-identification should be the default or *prima facie* position prior to any sharing.**

Biometric Data

73. The Law Council has considered the Bills in the context of biometric data, which can be described as an individual's physical characteristics (such as eyes and fingerprints) which can be used to verify their identity. The Law Council notes the immutable nature of biometric data and queries whether biometric data is specifically dealt with in the proposed legislation, as it is understood that such data is not considered differently from other data.

74. The apparent lack of specific reference to biometric data gives rise to questions about privacy safeguards. The data sharing regime is subject to other legislation, however, if biometric data is not so covered, then it is reliant on this regime, which is a risk management regime and relies largely on good will. The Law Council notes that under the Privacy Act, biometric information is defined and treated as a class of 'sensitive information'.[39] Specifically the definition of sensitive information includes 'biometric information that is to be used for the purpose of automated biometric verification or biometric identification' or 'biometric templates'.[40]

75. The Law Council considers the issue of consent, or lack thereof, in relation to the obtaining and subsequent sharing of such data to be a primary concern. In circumstances where biometrics are the only means of access to technology and buildings, and the data is subsequently available to be shared under this regime, the Law Council queries whether the persons subject to the biometric analysis are aware of the uses that may be made of their intimate data. This gives rise to a critical question as to whether the individual has provided meaningful consent to the use of their biometric data for external purposes, despite the fact that the purposes may be in the public interest.

76. The Law Council notes that sensitive information requires a higher standard of care, specifically where use of the information is a secondary use of such information.[41] Specifically, the Privacy Act provides that where an entity holds personal information

[38] Scrutiny Committee Report, 17.
[39] *Privacy Act 1988* (Cth) s 6 (definition of 'sensitive information').
[40] Ibid.
[41] *Privacy Act 1988* (Cth) sch 1 ('*Australian Privacy Principles*'): see Australian Privacy Principle 6.

that was collected for a particular purpose, it must not use or disclose the information for a secondary purpose without consent, subject to exceptions. An exception applies where the individual would reasonably expect the Australian Privacy Principle (**APP**) entity to use the information for the secondary purpose and, for non-sensitive personal information, the secondary purpose is related to the primary purpose. For personal information that is 'sensitive information' under the Privacy Act, the secondary purpose must be directly related to the primary purpose in order for the exception to apply.

77. The Law Council expresses concern at the perceived creation of 'mandatory consent' in these circumstances in the form of an agreement to share personal data in order to engage with an agency. Such situations render consent functionally meaningless. In the Law Council's view, where privacy interests that involve biometric data may be affected by the data sharing scheme, all sharing of such data should be based on prior express consent.

78. More broadly, the Law Council suggests that consideration be given to expanding the definition of biometric data under the Privacy Act to include all biometric data not only the biometric information that is to be used for the purpose of 'automated biometric verification or biometric identification' or 'biometric templates' as is currently specified.[42]

Recommendation:

- **The DAT Bill should be amended to provide that where privacy interests that involve biometric data may be affected by the data sharing scheme, all sharing of such data must be based on prior express consent.**
- **Consideration should be given to expanding the definition of biometric data under the *Privacy Act 1988* (Cth) to include *all* biometric data not only the biometric information that is to be used for the purpose of 'automated biometric verification or biometric identification' or 'biometric templates' as is currently specified.**

Sharing of data

79. Under the proposed scheme, sharing of information is not restricted to government bodies. Instead, the DAT Bill allows for private sector bodies to receive public sector information. This is of concern because the use of individual data by private companies presents a range of privacy concerns, as well as raising questions around issues of consent and how it is to be collected, monitored or enforced. Evidence shows that once people are made aware of how entities are collecting and using their personal information, they are much more likely to change their privacy settings.[43]

[42] For example, under the *General Data Protection Regulation,* biometric data means 'personal data resulting from specific technical processing relating to the physical, physiological, or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data': *General Data Protection Regulation* (European Union) art 4(14). Another example is that under Californian law biometric information means 'an individual's physiological, biological, or behavioural characteristics, including an individual's deoxyribonucleic acid (DNA), that can be used, singly or in combination with each other or with other identifying data, to establish individual identity': *California Consumer Privacy Act of 2018*, 1.81.5 Cal Civ Code § 1798.140(b).

[43] Attorney-General's Department, Australian Government, *Review of the Privacy Act 1988* (Issues Paper, October 2020) 44.

80. In relation to parameters around the sharing of data, the Scrutiny Committee has raised concerns as to why it is considered necessary and appropriate for guidelines on aspects of the data sharing scheme, which may play an important role in minimising the risk of interpretations of the operation of the scheme that trespass on personal privacy, to be included in non-legislative instruments that are not subject to parliamentary scrutiny.[44]

81. The Law Council shares this reservation, and notes that subclause 127(4) of the DAT Bill expressly states that these guidelines are not a legislative instrument. The Law Council is of the view that given the importance of the guidelines developed under the proposed scheme in setting the parameters for issues such as data sharing, these should be made by legislative instrument as therefore subjected to parliamentary scrutiny.

Recommendation:

- **Subclause 127(4) of the Data Availability and Transparency Bill 2020 (Cth) should be removed and a requirement should be inserted that Guidelines to be made by the National Data Commissioner are a legislative instrument and therefore subject to Parliamentary scrutiny and potential disallowance.**

82. Further, the Law Council highlights the concern raised by the Scrutiny Committee about the breadth of the 'unreasonable or impracticable' exception to the requirement to secure consent from an individual prior to sharing their personal information, especially noting the minister's advice that privacy interests will not be given priority in the public interest test.[45]

83. Based on this concern, the Scrutiny Committee has requested the Minister's further advice as to:

> *whether the addendum to the explanatory memorandum can provide specific examples of current guidance on the meaning of 'unreasonable or impracticable' and provide information on where this current guidance can be accessed.*[46]

84. The Law Council agrees that further guidance is needed in relation to the scope of practical application of the 'unreasonable or impracticable' exception as it applies to securing consent, noting that this should be a high threshold to obtain.

[44] Ibid.
[45] Scrutiny Committee Report, 17.
[46] Ibid.

Recommendation:

- **Further guidance is needed in relation to the scope of practical application of the 'unreasonable or impracticable' exception as it applies to securing consent, noting that this should be a high threshold to obtain and that many of the data sets collected are collected based on existing legal requirements or notices (not consents).**

Reliance on delegated legislation for accreditation

85. The Law Council shares the Scrutiny Committee's concern about the proposed reliance on delegated legislation to provide for procedures, requirements and matters relating to the accreditation of entities for the purpose of the data sharing scheme. The Scrutiny Committee explained that:

> *the Accreditation Rules will describe circumstances in which data custodians must use an accredited data service provider (ADSP) and specify documentation to support entities' claims against accreditation criteria. The minister advised that, as documents and circumstances for use of an ADSP are detailed and may change over time, this content is appropriate for rules. The committee further notes the minister's advice that significant matters will not be left to delegated legislation, as the weight of the accreditation framework is already located on the face of the bill, in Part 5.2.*
>
> *However, noting the importance of ensuring that the accreditation framework only permits accreditation of entities who can safely handle public sector data, from a scrutiny perspective, the committee remains concerned about the extent to which the [DAT Bill] relies on delegated legislation to determine matters related to the accreditation of entities under the scheme.*[47]

86. The Law Council recommends that these requirements be included in primary, rather than delegated, legislation to ensure these important matters receive the full benefit of Parliamentary scrutiny.

Recommendation:

- **Part 5.2 of the Data Availability and Transparency Bill 2020 (Cth) should be amended to provide greater detail in regard to the procedures, requirements and matters relating to the accreditation of entities for the purpose of the data sharing scheme.**

[47] Ibid 23.

Complaints mechanisms

Representative complaints

87. Part 5.3 Division 2 of the DAT Bill establishes a scheme for representative complaints to the Data Commissioner. As noted in the EM, all provisions are modelled off equivalent provisions from the Privacy Act.[48] The Law Council strongly supports the inclusion of a scheme of this form.

Merits review

88. Finally, the Law Council refers to the Scrutiny Committee's earlier concern about the:

> *appropriateness of the complaint mechanisms available to individuals whose privacy interests may be affected by the scheme, including the lack of mechanisms on the face of the bill to ensure that the National Data Commissioner has full visibility of privacy complaints made in relation to the scheme.*[49]

89. The Law Council acknowledges the Minister's statement that the DAT Bill's 'review and complaints mechanisms are scheme-specific to supplement existing redress mechanisms and reduce duplication and overlap' and that '[i]Individuals with concerns about the data sharing scheme will have access to existing complaints and administrative review processes'.[50]

90. However, the Law Council does not agree that individuals whose privacy interests may be affected by the data sharing scheme should not have access to merits review.

Recommendation:

- **Merits review should be available to individuals and their representatives (as individual or representative complaints) whose privacy interests may be affected by the data sharing scheme.**

[48] Explanatory Memorandum, Data Availability and Transparency Bill 2020 (Cth) [478].
[49] Ibid.
[50] Ibid.