Law Council
OF AUSTRALIA

Consumer Data Right Draft Rules

The Australian Competition and Consumer Commission

16 May 2019

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 2019 Executive as at 1 January 2019 are:

- Mr Arthur Moses SC, President
- Mr Konrad de Kerloy, President-elect
- Ms Pauline Wright, Treasurer
- Mr Tass Liveris, Executive Member
- Dr Jacoba Brasch QC, Executive Member
- Mr Tony Rossi, Executive Member

The Secretariat serves the Law Council nationally and is based in Canberra.

Acknowledgement

The Law Council is grateful for the contributions of the following organisations and Committees in the preparation of this submission:

- Queensland Law Society; and
- Privacy Law Committee of the Law Council's Business Law Section.

Executive Summary

1. The Law Council welcomes the opportunity to provide a submission to the Australian Competition and Consumer Commission's (**ACCC**) consultation on the Consumer Data Right (**CDR**) draft rules in the banking sector (**CDR draft rules**).

2. The Law Council has previously provided a submission to the Senate Standing Committee on Economics on the Treasury Laws Amendment (Consumer Data Right) Bill 2019 (**the Bill**). The Law Council notes that the Bill lapsed when the Federal Parliament prorogued with the announcement of the Federal Election on 11 April 2019.

3. The Law Council has also provided submissions on the draft Privacy Impact Statement for the CDR Rules in February 2019, on the Working Draft of the Consumer Data Standards in November 2018 and on the CDR Rules Framework in October 2018.

4. Generally, the Law Council supports the objects of these reforms to allow for greater access for consumers to their data. However, the Law Council holds concerns about the short timeframe within which it is proposed to finalise the CDR draft rules, with aspects of Opening Banking intended to be available from 1 July 2019. In addition, the Law Council notes that some of the necessary detail about the CDR draft rules will be clarified further in 'Data standards' which have not yet been made publicly available for public consultation. This difficulty is particularly acute in the absence of enabling legislation envisaged by the now lapsed Bill. There is no guarantee that the legislation will be so enacted on or before 1 July 2019.

5. The Law Council notes that there are significant privacy implications arising from these concerns and would urge reasonable consultation on all aspects of the reform prior to it being rolled out.

6. In this submission, the Law Council makes observations with respect to the CDR draft rules regarding:

    (a) the clarity of terms and offences;

    (b) valid requests and consents;

    (c) disclosure as to 'use' of consumer data;

    (d) the impact on consumers refusing consent to data being used for some purposes;

    (e) the storage of data; and

    (f) anonymity and data breaches.

7. The Law Council also reiterates some comments from its previous submissions regarding legislated privacy requirements and derived data as CDR data.

Consumer Data Right Draft Rules

Clarity of terms and offences

8. Proposed rules 3.5(1)(a) and 4.7(1)(a) provide that a data holder that has received a valid consumer data request made under Part 3 or Part 4 of the draft rules respectively, may refuse to disclose CDR data in response to the request, if it has reasonable grounds to believe that the disclosure would create a real risk of serious harm or abuse to an individual.

9. The Law Council is of the view that further clarity is required about the nature and scope of the 'serious harm or abuse' required for a data holder to refuse disclosure in response to a consumer data request. For example, clarity is required as to whether the threshold would be assessed against factors similar to those set out in section 26WG of the *Privacy Act 1988* (Cth) (**the Privacy Act**) for assessing the likelihood of serious harm, including consideration of the risks of CDR data disclosure as opposed to personal information. Ambiguity surrounding when a request should be refused may result in practical inconsistencies.

10. Clarity is also necessary to establish that the disclosure of the data was appropriate and to ensure that any obligations (as well as any potentially applicable civil penalty provisions) are easily understood by data holders. In addition, the relevant test to be applied requires careful consideration.

Valid requests and consents

Valid requests and consents

11. Proposed section 56BC of the Bill relates to rules about disclosure, collection, use, accuracy, storage, security or deletion of CDR data for which there are CDR consumers. The section provides:

    (1) Without limiting paragraph 56BB(a), the consumer data rules may include the following rules:

    (a) requirements on a CDR participant for CDR data to disclose all or part of the CDR data, in response to a valid request by a CDR consumer for the CDR data, to:

    (i) the CDR consumer for use as the CDR consumer sees fit; or

    (ii) an accredited person for use subject to the privacy safeguards;

    (b) rules about:

    (i) how a CDR consumer for the CDR data may make a valid request of the kind described in paragraph (a): and

    (ii) what must be included in a request for it to be valid, what disclosures or other matters a valid request may cover, and when a request ceases to be a valid request:

12. Despite proposed paragraph 56BC(1)(b) of the Bill, the CDR draft rules do not provide sufficient guidance in proposed rules 3.3 and 4.3(4) regarding the requirements of a

'valid request'. From both a consumer and privacy perspective, this is both concerning and raises some further practical issues in terms of implementation.

13. In particular, guidance regarding what should be included in the request for it to be valid should be articulated in the CDR draft rules to ensure that CDR data is protected and that the appropriate compliance steps have been undertaken prior to data being shared or used.

Consents

14. Proposed rule 4.10(1)(a) provides that 'a consent given by a CDR consumer to collect CDR data' must be 'voluntary'. The Law Council suggests that it would be appropriate to expand on this requirement and expressly state that an accredited person must not offer to provide goods or services, or offer to provide goods or services at a particular price (i.e. offer a discount), on the condition that a consumer provides a consent to collect CDR data. The Law Council submits that this would prevent situations where a service provider attempts to impose a condition that a consumer give them visibility of data held by another service provider.

15. Secondly, reference is made in proposed rule 4.10(2)(d) to the 'data standards'. Division 8.4 indicates that these data standards have not yet been made. The Law Council submits that further information needs to be provided to guide the consent process to protect vulnerable consumers from consenting to the access of CDR data unknowingly. It must also provide accredited data recipients with a clear understanding of their obligations of disclosure. In particular, where, for example, the use or disclosure of CDR data for direct marketing by accredited data recipients without a 'valid consent' is proposed to be a civil penalty provision in the Bill under proposed section 56EJ.

Disclosure as to 'use' of consumer data

16. The Law Council notes that proposed rules 1.7 (data minimisation principle) and 4.4 refer to the use of CDR data by an accredited person being limited to 'what is reasonably needed in order to provide goods and services under a CDR contract'.

17. Under proposed rule 4.10(3), when an accredited person is asking a CDR consumer to give their consent to collect CDR data, the accredited person must:

    (a) identify the types of CDR data for which the consent is sought, having regard to the data minimisation principle;

    (b) allow the CDR consumer to actively select or actively specify which types of CDR data they are consenting to the accredited person collecting; and

    (c) ask for the CDR consumer's express consent for the accredited person to collect the selected or specified data.

18. Under proposed rule 4.10(4), the accredited person must give the CDR consumer the name and contact details of the accredited person and how long the accredited person is asking CDR consumer to give their consent (i.e. for a single collection of CDR data or collection of CDR data over a period of time of not more than 12 months). If the consumer is being asked to give a consent for collection over a period of time, the accredited person must tell the CDR consumer what that period is and how often data is expected to be collected over that period. The accredited person must also give the CDR consumer the period for which the accredited person would hold the CDR data

that is the subject of the consent and a statement that at any time, the consent can be withdrawn, and instructions for how the consent can be withdrawn.

19. The Law Council submits that proposed rules 4.10(3) and/or (4) should go further by providing both:

    (a) an explicit obligation on the accredited person to disclose how the data will be used; and

    (b) a prohibition on the accredited person using the data for any purpose not disclosed at the time at which consent to collect the data was given.

20. This would also serve to increase the level of information available to a consumer when they are deciding whether to consent to the collection of their data and may also simplify the consumer's dealings with the accredited person.

Impact on consumer refusing to consent to data being used for some purposes

21. Proposed rule 4.16(3) details the obligation of an accredited person to allow the CDR consumer to select or specify the uses of the data they are consenting to. In order to protect consumers from a position where goods or services are refused on the basis that a consent is limited, the Law Council considers it is appropriate to include an additional obligation on the accredited person so that consumers effectively have the right to withhold consent to particular use(s) of their data.

22. This would be to the effect that an accredited person must not refuse to provide goods or services to consumers on the basis that the consumer did not give consent to a specific use of their data where it is not necessary in order for the relevant goods or services to be provided.

Storage of data

23. Proposed rule 4.16(6)(c) provides that if CDR data is disclosed to an outsourced service provider, including one that is overseas, that the CDR consumer should be given that information.

24. The Law Council considers that it might also be appropriate to include an additional sub-rule to provide that the accredited person must also disclose to the CDR consumer if CDR data is to be stored by an overseas provider generally, not just by an outsourced provider.

25. Proposed rule 7.2(2)(a) provides that in addition to the information referred to in subsection 56ED(5) of the Bill, an accredited data recipient's CDR policy must, among other things, include a list of the outsourced service providers (whether based in Australia or based overseas, and whether or not any is an accredited person). The Law Council considers that this rule should also be similarly expanded to require transparency where accredited data recipients propose to disclose, access, store or otherwise process data overseas. The Law Council notes that the term 'disclosure' has a particular meaning under the relevant regulatory guidance. In particular, careful consideration should be given to what constitutes 'effective control of the data', in the event of cross border flows. This has been the subject of some debate and will require alignment with existing provisions of the Privacy Act and relevant regulatory guidance.

Anonymity and data breaches

26. Proposed subsection 56EE(1) of the Bill provides that an accredited data recipient of CDR data must give each CDR consumer for the CDR data the option of using a pseudonym, or not identifying themselves, when dealing with the accredited data recipient in relation to the CDR data. Proposed section 56EE includes a note that the CDR participant from whom the accredited data recipient acquired the CDR data may be subject to a similar obligation under Australian Privacy Principle 2.[1]

27. Proposed subsection 56EE(3) of the Bill provides that subsection 56EE(1) does not apply in the circumstances specified in the CDR rules. These circumstances are spelt out in proposed rule 7.3. and are when:

    (a) the accredited data recipient is required or authorised by law or by a court/tribunal order to deal with an identified CDR consumer in relation to particular CDR data; or

    (b) in relation to particular CDR data, it is impracticable for the accredited data recipient to deal with a CDR consumer that has not been identified.

28. The Law Council is concerned about the practical effect of rule 7.3(b) and the need to ensure that consumers are aware that data may not be anonymously provided. In the view of the Law Council, if the accredited data recipient is unable to provide anonymity or the use of pseudonyms, the consumer should be advised prior to obtaining consent to disclose or use the data in any way.

29. Finally, the Law Council notes that proposed section 56ES of the Bill relates to 'Notification of CDR data security breaches' and that Part NIC of the Privacy Act is to apply to an accredited data recipient or designated gateway who holds consumer data. As currently drafted, it would appear that notification would only be provided to the consumer if the 'access, disclosure or loss' was 'likely to result in serious harm'.

30. In the view of the Law Council, given the significant privacy implications arising from the proposed reforms, it would seem appropriate to also include a positive obligation (within proposed rule 7.8, for example), requiring accredited persons or data holders to inform consumers of any security breach (including, for example, any unauthorised access or inadvertent disclosure) of CDR data which may affect them.

Ongoing concerns of the Law Council

Legislated minimum privacy requirements

31. The Law Council notes Division 7.2 of the CDR draft rules which relate to privacy safeguards.

[1] Australian Privacy Principle 2 relates to anonymity and pseudonymity. It provides that individuals must have the option of not identifying themselves, or of using a pseudonym, when dealing with an APP entity in relation to a particular matter except in particular circumstances (the APP entity is required or authorised by or under an Australian law, or a court/tribunal order, to deal with individuals who have identified themselves or it is impracticable for the APP entity to deal with individuals who have not identified themselves or who have used a pseudonym).

32. In the Law Council's submission on the Exposure Draft of the Bill, it noted that personal information will be a subset of CDR data, the handling of which is already regulated under the Privacy Act.[2] The Law Council expressed concern that the current drafting of the Bill would empower the ACCC to override and undermine the protections of the Privacy Act in respect of CDR data and by implication of personal information.

33. In its previous submission, the Law Council suggested that it would be beneficial to legislate minimum privacy requirements that cannot be derogated from by the CDR rules, for example minimum storage and security requirements, minimum reporting and record keeping requirements, and a basic framework for the accreditation process. It was suggested that consumer credit reporting information, as regulated under Part IIIA of the Privacy Act, would also need to be expressly addressed.[3]

34. The Law Council recognises that the Privacy Safeguards articulated in the Bill and further addressed in the CDR draft rules go further than the Australia Privacy Principles in the Privacy Act in certain respects, in particular regarding the threshold for consent and data security requirements. The Bill creates a 'minimum set' of Privacy Safeguards for the CDR, which the Office of Australian Information Commissioner has described as 'more restrictive and… more details than their equivalent APPs'.[4] However, the Law Council reiterates the point raised in paragraph 4 above that the current absence of the enabling legislation is a fundamental flaw in the CDR regime.

35. The Law Council reiterates that segregating the regulation of privacy (including the APPs and privacy safeguards) between the Office of Australian Information Commissioner and the ACCC in relation to CDR data and personal information will likely result in confusion for consumers. The Law Council is of the view that if the structure of the Bill remains in its current form, a comprehensive public education campaign will need to be conducted to minimise that likely confusion.

'Required consumer data'

36. In the Law Council's submission on the Bill, the Law Council noted that proposed paragraph 56AI(1)(a) provides that CDR data is information that is within designated class, as described in the Ministerial instrument or data, that is not so covered but is wholly or partly derived from information covered by paragraph (a) of this subsection. Notably, there is no limit specified as to the extent of derivation. The Law Council considers that there must be some class-closing rules: otherwise there may be the risk that distant derivations, such as bank divisional reports and other aggregations and transformations of data, could be subject to the CDR.

37. The Law Council submitted that by current provisions of the Bill it is left to the Ministerial designation to create class closing rules, or to the CDR rules as promulgated by the ACCC to describe what the Minister intended.

38. Part 2 of Schedule 2 of the CDR draft rules relates to CDR data that may be accessed under these rules in relation to the banking sector. As per proposed rule 2.1, 'required

---

[2] Law Council of Australia, Submission to Senate Standing Committees on Economics, *Treasury Laws Amendment (Consumer Data Right) Bill 2018* (27 February 2019).
[3] Noting that Part IIIA already excludes the APPs in respect of credit information, and are (for most purposes) more prescriptive than the Privacy Safeguards, and therefore it is likely that in dealing with credit information that is also CDR data, the entity would solely need to comply with Part IIIA unless requirements of Part IIIA are expressly addressed or overridden by an effective legislative instrument.
[4] The Treasury, *Consumer Data Right Privacy Protections* (2018) <https://static.treasury.gov.au/uploads/sites/1/2018/12/CDR-Privacy-Summary.pdf>.

product data' in relation to the banking sector, for the purposes of the CDR draft rules, means CDR data:

(a) that is primary CDR data;
(b) for which there are no CDR consumers;
(c) that is about the eligibility criteria, terms and conditions, price, availability or performance of a product;
(d) in the case where the CDR data is about availability or performance—that is publicly available;
(e) that is product specific data about particular products; and
(f) that is held in a digital form.

39. As per proposed rule 2.1, CDR data is 'required consumer data' in relation to the banking sector for a consumer data request made by or on behalf of a particular CDR consumer at a particular time if:

(a) the data is primary CDR data; and
(b) the data is:
    (i) customer data in relation to that consumer; or
    (ii) account data in relation to an account held by that consumer:
        (A) in their name alone; or
        (B) if the person is an individual—jointly with 1 other individual; or
    (iii) transaction data in relation to a transaction relating to such an account; or
    (iv) product specific data in relation to a product that the consumer uses; and
(c) the data is held by the data holder in a digital form; and
(d) the consumer is, at that time, able to access products of the data holder online, for example, using an internet browser or a mobile phone application; and
(e) the consumer has an account with the data holder that:
    (i) is active when the request is made; or
    (ii) is not active at that time, but was closed on or after 1 January 2017.

40. Proposed rule 2.2 states that 'required consumer data' does not include derived data. In doing so, the Law Council notes that in relation to designated CDR data for Open Banking, the definitions exclude derived data. This assists with clarity as to the scope of 'required product data' and 'required consumer data'. However, derived data may still, technically, be within scope for other designated industries. This is an important matter of scope that requires attention. To that end, the Law Council notes that this issue is best addressed under the Bill or, as a minimum, subject to transparent and certain rules applicable to the scope of the decision making of the relevant regulator, in this case the ACCC.