Treasury Laws Amendment (Consumer Data Right) 2018 Bill

Australia

Data Governance

Definitions of Data:

N/A

Main Focus of Document:

Protection and management of data for citizens and persons doing business in Australia. This is a Bill for an Act to amend the law which relates to fair trading, competition, consumer protection and privacy.

Target Beneficiaries or Sectors:

Australians and persons doing business in Australia

Key Elements:

The Consumer Data Right (CDR) covers both competition and consumer matters, as well as privacy and confidentiality concerning the use, disclosure and storage of data. The CDR 'provides individuals and businesses with a right to efficiently and conveniently access specified data in relation to them held by businesses. The CDR authorises secure access to this data by trusted and accredited third parties. The CDR requires businesses to provide public access to information on specified products they have on offer. CDR is designed to give customers more control over their information leading, for example, to more choice in where they take their business, or more convenience in managing their money and services'.

Legislation The CDR will be established primarily through amendments to the Competition and Consumer Act 2010 and the Privacy Act 1988. This enabling legislation will: • set out the role, functions and powers of each of the ACCC, OAIC and Data Standards Body; • outline the overarching objectives and principles for the Consumer Data Right; • create a power for the Treasurer to apply the Consumer Data Right to new sectors; and • enshrine a guaranteed minimum set of privacy protections, which will be built upon in the ACCC rules. The Treasurer will consult on draft legislation in the coming months.

Sectoral assessment and designation The Government has decided that banking will be the first sector the CDR will apply to, where it will be known as Open Banking. Open Banking will be followed by application of the CDR to the energy and telecommunications sectors. Future sectors of the economy which will become part of the CDR will be identified through sectoral assessments conducted by the ACCC. The ACCC may initiate a sectoral assessment on its own initiative or at the request of the Treasurer. Following a sectoral assessment, the ACCC will advise the Treasurer on whether to designate a sector. The OAIC will aid the ACCC in its assessment and will also advise the Treasurer regarding the privacy impacts of designating a sector.
The Treasurer will then determine whether to designate a sector. Under that process, the Treasurer will determine, on advice from the ACCC and OAIC, whether the benefits of designating a sector outweigh the costs. This would involve consideration of: • likely impacts upon consumers; • likely impacts upon relevant markets, including upon market efficiency, integrity and safety; • likely impacts upon privacy for individuals and confidentiality for businesses; • likely regulatory impact of consumer data rules; and • any other relevant matters. In particular, in considering a designation, the Treasurer would have regard to the promotion of competition and data driven innovation in the Australian economy. A ‘sector’ designation is more specifically a designation of the classes of entity and data in relation to which the right will apply; and may not align with what is traditionally considered an industry sector. The enabling legislation will set out these processes and the criteria which the Treasurer must consider when making a designation.

Breaches of the Consumer Data Right The ACCC will also have a general strategic enforcement role where there are repeated or serious breaches. Given that data breaches may occur in the course of activities regulated by other agencies (e.g. consumer credit provision or financial services), other sector specific regulators may be best placed to respond to a given concern. Consumers will also have standing to directly sue if their rights under the CDR have been breached. Remedies available from regulators where data holders or recipients have breached the CDR rules will include infringement notices, civil penalties, compensation orders, enforceable undertakings and de-accreditation of data recipients (or suspensions or imposition of conditions), depending on the circumstances. Injunctions (court orders compelling an entity to do or refrain from doing specified activities) will also be available, including orders for the deletion of data. Assistance from the OAIC and external dispute resolution schemes will not be available to large business customers. The ACCC-made rules may provide for other dispute resolution arrangements for them. They will, like all consumers under the system, have access to direct rights of action.

Data protection and privacy Privacy and security are core features of the CDR. To protect the privacy of consumers, privacy protections will be strengthened and tailored to adequately reflect the needs of the CDR and each sector. These privacy protections will include: • requirements that data can only be transferred under the CDR at the direction of the consumer • requirements for greater transparency and choice so that consumers control how their information will be used • the mandatory accreditation of data recipients • obligations regarding deletion of data • the introduction

of transfer, security and data standards via a newly created Data Standards Body (initially Data61) • extension of Privacy Act 1988 protections to bind all accredited data recipients, including small to medium sized enterprises • a strong role for the Office of the Australian Information Commissioner (OAIC) in advising on and enforcing privacy protections • a range of avenues for consumers to seek meaningful remedies for breaches, including external dispute resolution and direct rights of action The legislative framework will establish clear principles of liability to ensure that there is no uncertainty about the rights and liabilities of consumers, data holders or data recipients.

Safe and controlled use of data Data will only be transferred to third parties at the direction of the consumer. Separate to the direction to transfer (given to the original data holder), consumers will need to give consent for how the data will be used (given to the data recipient). Consumers will be free to determine what their data is used for. It is not proposed that consumers will be prohibited from granting consent to any lawful uses. The CDR will specify requirements regarding the consent giving process to ensure that consumers are properly aware of and understand what they are consenting to. Certain high risk uses may require separate consents to be obtained by the data recipient. It is currently proposed that these uses will be: • use of the data for marketing; • on-sale of the data; • transfers of the data overseas; and • transfers of the data out of the CDR system to a party who is not subject to its enhanced privacy and data security regime.

Consumer Consent The CDR is a right for consumers to choose to safely share their data with accredited, trusted recipients. It is not a right for businesses to share consumer's data without their consent. The system will ensure that consent is genuine – that consumers understand what they are consenting to, that consents are clear and unambiguous, and they are not open ended. There will be no 'implied' consent allowed for data transfers. Consumers will be able to keep track of consents to share data and will be able to revoke them. Records of consents will themselves be designated data-sets under the CDR, opening the possibility of external service providers assisting consumers to keep track of what they have agreed to. Rigorous consent requirements will apply to both the transfer of data and the subsequent use of data under the system.

Competition Consent Data Data privacy Data protection Data security Data standards Data transfer or transmission Innovation Legislative framework Transparency

Policy/regulation mirrored:

N/A

Countries: