Australian Government
The Treasury

TSY/AU

Consumer Data Right Privacy Protections

December 2018

Manager
Media and Speeches Unit
The Treasury
Langton Crescent
Parkes ACT 2600
Email: medialiaison@treasury.gov.au

The Consumer Data Right impacts upon privacy in two primary ways

The right of an individual to access data about themselves is recognised to be a core privacy right. The Consumer Data Right grants additional access rights to those contained in Australian Privacy Principle 12, in relation to designated data sets. This new access right has greater functionality, more security and may apply to different kinds of data than existing privacy rights.

The Consumer Data Right also enables individuals to give direct access to their data to third parties. This may also be considered to be an extension of privacy rights. Additionally, in relation to this third party data access, the reforms impose an enhanced privacy framework beyond that which would ordinarily apply, directed at preventing inappropriate collection, disclosure, holding and use of data.

Targeted application

The Consumer Data Right is only applied to data sets after consideration of privacy impacts has taken place.

Going forward, data sets and data holders will only become subject to the Consumer Data Right following detailed sectoral assessments by the ACCC, in conjunction with the OAIC.

The Treasurer must then consider (amongst other things) the privacy and confidentiality impacts before designating a sector as subject to the right.

The Treasurer may make regulations to accompany a designation, to ensure that the ACCC made Consumer Data Rules (Rules) contain (or do not contain) certain requirements, including in relation to privacy.

In respect of banking data sets, the Open Banking Review carried out the equivalent of the proposed ACCC sectoral assessment process. The transitional provisions of the Bill dispense with the requirement for an additional sectoral assessment for the banking data sets being designated.

A voice for privacy

The Office of the Australian Information Commissioner (OAIC) will act as a source of expertise and advocacy for privacy protection.

The OAIC will be an active participant in sector designation, rulemaking and standard setting under the regime. The first two roles are provided for in the Bill, with the latter to be addressed through the Rules and their observer status with the Data Standards Body.

The OAIC must be consulted by the ACCC in relation to sector designation and rulemaking. The OAIC may also independently advise the Treasurer on whether to issue a designation or consent to a rule. The OAIC may make these advices publicly available.

The ACCC must undertake public consultation in relation to sector designation and rule-making. In respect of Rules for the banking sector, the transitional provisions of the Bill dispense with the requirement for additional consultation as the ACCC will consult on draft Rules before the Bill is passed.

Privacy Safeguards

Strong minimum privacy protections for collection, disclosure and use

The Bill will create a minimum set of Privacy Safeguards for the Consumer Data Right.

Each *Australian Privacy Principle* will have its equivalent but more onerous Privacy Safeguard. The exception to this is APP12 *Access to personal information*, for which the entirety of the Consumer Data Right is the enhanced equivalent.

The Privacy Safeguards, while generally consistent with the APPs, are more restrictive and, in conjunction with supporting Rules, will be more detailed than their equivalent APPs. They will have broader application, to catch all designated data relating to identifiable natural and legal persons and to bind all accredited data recipients in respect of CDR data they've received. To minimise the complexity of the CDR regime, most of the Privacy Safeguards will not apply to data holders. Data holders will instead be subject to the *Privacy Act 1988* (Privacy Act).

These stronger protections mitigate risks associated with more convenient and higher velocity transfers of valuable machine readable data; and to instil justified high levels of consumer confidence in the use of the system.

The Privacy Act has a general civil penalty (up to 2000 penalty units and five times that for corporations) only for serious or repeated breaches of privacy, which can apply to breaches of any APP.[1] Breaches of most Safeguards attract civil penalties, with no requirement for breaches to be serious or repeated – with penalties capped at the greater of, for individuals, $500,000 or, for corporations, $10,000,000; three times the total value of the benefits that have been obtained; or 10% of the annual domestic turnover of the entity committing the breach. This aligns with competition and consumer law penalty amounts.

Further Privacy Protections

The Privacy Safeguards set the minimum protections.

In addition to Privacy Safeguards hardwired into the primary legislation, the framework provides flexibility to respond to emerging privacy risks, through rulemaking and standard setting processes.

The ACCC may make additional Rules regarding the transfer, holding and use of data within the system, to build upon the Privacy Safeguards.

The Data Standards Body may make technical standards to support the operation of the Privacy Safeguards and any further protections in the Rules – for example, information security standards.

Breaches of more specific Rules in addition to any Safeguard can attract civil penalties up to an amount specified in the Rules, capped at the greater of, for individuals, $500,000 or, for corporations, $10,000,000; three times the total value of the benefits that have been obtained; or 10% of the annual turnover of the entity committing the breach.

There are also other aspects of the CDR legislation that help to protect privacy. For example, a CDR designation instrument for a sector may provide that a particular intermediary is a designated gateway for that sector. Data holders may then be required to transfer data through that designated gateway. Designated gateways will only be able to collect, use and disclose information as specifically provided for in the Rules.

[1] A penalty unit is currently $210

Genuine consent

Consents to collect, disclose, hold or use will need to be genuine.

The Consumer Data Right will provide consumers with the right to access data relating to them held by a business; or to direct that it be transferred to a trusted third party.

The Open Banking Review proposed that the ACCC rulemaking should ensure that consent under the regime is genuine. It is intended that the Rules will set out requirements to ensure that consent is express, informed, current, clear, specific, unbundled and time limited. The Rules will ensure that consent must be given by the relevant people and by those with appropriate capacity. The Rules will be able to set requirements for the processes for obtaining consent.

The Rules relating to consent will be developed by the ACCC in consultation with the OAIC, having regard to real world behaviours of consumers and based upon evidence of the actual efficacy of existing consent processes.

A 'data safety licence'

Data transfer will only be permitted to trusted data recipients

Within the CDR system, the Consumer Data Right will generally only permit data relating to identifiable consumers to be transferred to *accredited* data recipients (or the consumer themselves).

Transfers of data out of the CDR system will be possible, but highly restricted.

The ACCC will be responsible for data recipient accreditation. Accreditation will be directed at ensuring that the data recipient is a person who can be trusted to receive, hold and use data. The accreditation criteria will be set out in the Rules and are expected to include information security, privacy, fit and proper and identity verification requirements.

It is expected that there will be graduated tiers of accreditation, with high risk data and uses requiring stronger protections to be in place.

It is expected that the Rules will put in place requirements for data holders to verify the identity and accreditation status of third parties before releasing data.

It is expected that technical standards will require arrangements to be put in place that automatically block access to non-accredited entities. Communications will be required to be encrypted.

The ACCC will be empowered to suspend, revoke, downgrade or impose conditions upon accreditations.

Data recipients must also be bound by the Privacy Act.

Generally, small to medium sized enterprises are not bound by the Privacy Act.[2]

The Bill provides that this exception is not available to enterprises that obtain accreditation to receive data under the Consumer Data Right. This means that the Privacy Act will apply to information for which the Privacy Act would otherwise apply (other than Consumer Data Right Data, in relation to which the Privacy Safeguards will instead apply). The Safeguards will protect Consumer Data right data held by accredited data recipients.

[2] The Privacy Act 1988 defines SMEs as businesses with annual turnovers of less than $3 million.

Rights to withdraw or delete

There will be rights to withdraw consent to disclosures and use of data

Consumers will be entitled to withdraw their consent to a data holder providing access to a data recipient.

The Rules will be able to provide for circumstances in which consumers will be entitled to withdraw a consent previously given to a data recipient for them to use the consumer's data.

The Bill will require data to be deleted or de-identified upon any use permissions becoming spent. This will operate in conjunction with the requirement for all use permissions to be express and specific.

Dual regulator model

Regulators will play to their strengths

The OAIC will be empowered to provide individual remedies, in conjunction with external dispute resolution arrangements. They will have primary responsibility for enforcing the Privacy Safeguards but may also be delegated enforcement functions relating to the Rules, to support their role.

The ACCC will have a strategic enforcement role (bringing their greater litigation resources and experience to bear), focusing on consumer and competition outcomes. They will have primary responsibility for enforcing the balance of the regime, but may also be delegated enforcement functions relating to the Privacy Safeguards.

Between the regulators, there will be a no-wrong door approach to consumer complaints.

There will be a graduated and powerful set of regulatory tools.

The Bill provides regulators with extensive powers:

- Criminal penalties
- Civil penalties
- Compensation orders
- Infringement notices
- Injunctive orders
- Disqualification of directors orders
- Adverse publicity orders
- Enforceable undertakings
- Investigation and auditing powers
- Sectoral assessment/general inquiry powers
- Information sharing

There will be new criminal penalties for misleading consumers into believing that a data recipient is accredited (or accredited to a level that they are not). There will also be new criminal penalties for misleading consumers that they are using the CDR data sharing system when they are not.

The Bill will extend the Privacy Act breach reporting regime to breaches of the CDR Privacy Safeguards and associated rules.

Resourcing

Strong protections will be backed by well-resourced regulators

The OAIC and other agencies have been granted significant funding to develop, set and enforce privacy protections as part of the Consumer Data Right.

In the 2018-19 Budget, the Government announced that it will provide $45 million and 45 ASL to fund regulators over the next four years.

$ millions	2018-19	2019-20	2020-21	2021-22	Total
ACCC	5.2	5.1	4.9	5.0	**20.2***
OAIC	3.6	3.2	3.0	3.1	**12.9***
CSIRO-Data61	3.7	2.9	2.5	2.5	**11.5***
Total Impact on Underlying Cash:	**12.5***	**11.2***	**10.4***	**10.5***	**44.6***

ASL	2018-19	2019-20	2020-21	2021-22
ACCC staff	19.0	23.0	23.0	23.0
OAIC staff	10.0	15.0	15.0	15.0
CSIRO-Data61 staff	11.4	8.3	6.7	6.7
Total staff	**40.4**	**46.3**	**44.7**	**44.7**

Funding has been included to facilitate consumer and privacy advocate participation in standards setting processes.

In the 2018-19 Mid-Year Economic and Fiscal Outlook, the Government provided additional funding for the ACCC to implement new systems and processes to support the rollout of the Consumer Data Right. The figures are not for publication due to commercial sensitivities.

*Figures may not sum due to rounding

External dispute resolution

There will be accessible and meaningful remedies.

Consumers will have access to external dispute resolution arrangements, leveraging off existing sector specific schemes. The OAIC will also be empowered to provide remedies to individuals (and small and medium sized enterprises).

While, generally, the enhanced protections will apply to all data and bind all parties handling data within the system, only individual and small to medium sized enterprise customers will have access to external dispute resolution schemes and OAIC assistance.

Direct rights of action

Private remedies – individually or collectively

A breach of the Privacy Act does not give rise to a direct right of action for compensation by an aggrieved party against the person committing the breach.[3]

The Consumer Data Right Bill provides a direct right of action for breaches of the Consumer Data Right. One or more breaches affecting multiple parties may support a class action.

These rights will exist in parallel to any rights to alternative dispute resolution, and the ability for the ACCC and OAIC to grant remedies[4].

Education

Informing consumers of their privacy rights and remedies

The 2018-19 Budget provided both the ACCC and OAIC with funding to conduct ongoing education of consumers regarding the Consumer Data Right.

Data61 has been provided with funding for the education of data holders and recipients, including in relation to compliance with technical standards directed at privacy, confidentiality and information security.

The legislation empowers the OAIC to issue guidance regarding the Privacy Safeguards.

Coverage

A broader range of data is caught by the CDR and subject to its privacy protections

The Consumer Data Right framework – including its privacy and confidentiality protections - can potentially apply to data that *relates* either to a natural or legal person.[5] The Privacy Act generally applies to the narrower class of data that is *about* an identified or reasonably identifiable natural person.

A broader range of people benefit from the CDR and its protections

The Consumer Data Right is exercisable by both natural and legal persons, including small and medium sized enterprises.

A broader range of people can be obliged to provide protections

The Consumer Data Right framework may apply to all data holders covered by a Ministerial designation. Additionally all persons who apply for and obtain accreditation as a data recipient will also be subject to the scheme. It may therefore apply to small and medium sized enterprises, which are not generally caught by the Privacy Act.

The application of the Privacy Act is also extended to persons who hold accreditation, in relation to non-consumer right data.

It applies to Australian entities and Australian data

Overall, the potential jurisdictional reach of the Consumer Data Right is also broader than that of the Privacy Act.

---

[3] The Privacy Act does, however, allow an individual to seek injunctive relief through the courts. Some direct rights of action may arise from the relevant conduct under other laws, such as defamation laws, breach of contract or consumer laws regarding misleading and deceptive conduct.

[4] The OAIC is limited to providing remedies to individuals and small and medium sized enterprises.

[5] Only when that type of data is designated as being subject to the regime.

Privacy Protections at Each Stage