

Third Party Data Policy

The Office of State Revenue, through the Risk, Analytics and Finance Division, confidentially acquires data from a range of third party providers, including other State and Commonwealth agencies. Third party data is used for the purposes of administering and enforcing taxation, revenue and grant laws.

1. Purpose

The purpose of this policy is to outline the lawful and appropriate use of third party data across the Office of State Revenue (OSR). This policy takes into account the legislative limitations relating to the acquisition and disclosure of confidential information, as well as other privacy and secrecy requirements. This policy also considers the legally binding requirements placed on the Commissioner of State Revenue through the various third party agreements, whether formal or informal, including memoranda of understanding, where applicable.

2. Background

To ensure consistency of use of third party data in accordance with relevant legislation, agreements and other obligations, consideration must be given to the purpose for which each third party dataset is acquired, the permissible use of the dataset, as well as any other relevant considerations, such as reputational risk to the commissioner, that may arise in the course of considering each instance of proposed use of third party data.

The responsibility for acquiring third party data and determining permissible use of each third party dataset resides with Risk, Analytics and Finance Division, Business Intelligence Unit ("BI"). From time to time, legal advice may be sought in order to clarify the Commissioner's position on the above. Requests for clarification are to be directed to BI for consideration and progression, if necessary. BI maintains a library of legal advice and other interpretive material relating to the acquisition and use of third party data.

This policy is provided as guidance for all OSR staff, including permanent, temporary staff and contractors, and is intended to outline the obligations and responsibilities of staff when requesting, using and communicating to others about third party data.

3. Confidentiality

All OSR staff are required to comply with the confidentiality and collection of information provisions as outlined in Part 8 of the *Taxation Administration Act 2001*. Key points to be aware of include:

Confidential information means information disclosed to, obtained by, or otherwise held by, an official under or in relation to a tax law.

An **official** means a person who is, or has been, a public service employee or other person, performing functions under or in relation to the administration or enforcement of a tax law.

- **An official must not disclose confidential information to anyone else other than under [Part 8]:** (s.111(1))
- **If a person receives confidential information that the person knows, or ought reasonably to know, is confidential information, the person must not disclose the information to anyone else unless the disclosure is permitted under [Part 8]:** (s.112(1)(b))
- **The maximum penalty for breach of either of the two provisions above is 100 penalty units (currently \$13,055).**



Personal confidential information, for a person, means confidential information that identifies, or is likely to identify, the person, or discloses matters about the person's affairs.

Reference to a **person** includes reference to a corporation as well as an individual.

The **commissioner may** disclose personal confidential information to the extent necessary to perform the commissioner's functions under or in relation to the administration or enforcement of a tax law or another law administered by the commissioner.

Governance over the purpose of acquisition and use of third party data may be further restricted by other legislation, information privacy principles and specific agreements.

4. Restrictions on naming third party data providers

Third party data is a general term to describe all non-OSR data sources, including bulk data and lookup services. As the term *third party data* is all encompassing, it supersedes the terms *external data* and *CAV data*.

When communicating with clients or colleagues, either in writing or verbally, OSR officers must not reveal any information about the specific data used or the name of the third party data provider. For example, you may say 'based on third party data' or 'matched with third party data' but you cannot say 'according to the ATO' or 'based on data from ASIC'.

Third party data providers should not be named in any correspondence whatsoever. All information, including for the purposes of educational material or client seminars, may only broadly reference *third party data* but must not disclose the data provider or methods used to analyse the data.

If there are special circumstances where there may be a need to provide more details to a client or other person, director approval is required prior to raising with BI for determination of the appropriate course of action.

Appendix 1: Examples of third party data acquired by OSR

OSR acquires data from a range of third party providers. How each data set can be lawfully used is determined by Queensland and Commonwealth legislation, Information Privacy Principles, Commissioner's practice and, where applicable, through formal agreements. As a result, there are no blanket rules for determining appropriate use of third party data, and each matter must be considered on a case by case basis.

Examples of third party data providers may include:

- Australian Taxation Office (ATO)
- Australian Business Register (ABR)
- Australian Securities and Investments Commission (ASIC)
- Department of Employment, Small Business and Training (DESBT)
- Department of Transport and Main Roads (TMR)
- Electoral Commission of Queensland (ECQ)
- Residential Tenancies Authority (RTA)
- WorkCover Queensland (WCQ)

Appendix 2: Usage of third party data

Data is acquired through relevant legislative provisions and formal arrangements such as memoranda of understanding (MOU). How each data set may be used is determined by the conditions of the relevant acquisition process. As an example, OSR receives monthly data from ECQ. Consistent with our agreement with ECQ, we may use this data to conduct single look ups for an individual's contact details. However, we may not use the data to match against multiple records.

For more information on authorised functions and uses of third party data, OSR officers should contact the Manager, Business Intelligence or Director RAF. All requests for third party data need to be approved for a specific purpose before data will be provided. If you intend to use third party data for a different purpose, even if you already have access to the data, you will need to have your director's approval who will then refer to RAF Division for review and approval where appropriate.

Appendix 3: Supporting references

The following references may provide further guidance for the use of third party data:

- Fines for breaching EU General Data Protection Regulation (GDPR) ([link](#))
- Third Party Data Info page, with MOU and agreements ([link](#))
- Third Party Data file request overview ([link](#))