DGA

DATA GOVERNANCE AUSTRALIA

Draft Code of Practice

FOR PUBLIC CONSULTATION

Foreword

Data Governance Australia "DGA" is committed to setting industry standards and benchmarks for the responsible and ethical collection, use and management of data in Australia. We are developing a Code of Practice as part of our ongoing effort to set leading industry standards, promote a culture of best practice, as well as to drive innovation by increasing consumer confidence and trust in the data-practices of organisations.

The DGA Code of Practice is a principles-based self-regulatory regime that sets leading industry standards and benchmarks for responsible and ethical data-practices. The DGA Code of Practice will be enforced by an independent Code Authority, which consists of seven members – 3 members from consumer groups, 3 members from industry, and an independent Chair.

DGA has developed this Draft Code of Practice through extensive consultation with 12 major Australian corporations since 4 October 2016, when the creation of DGA was first announced. These corporations represent a wide cross-section of industry and a range of data practices. We are releasing this Draft Code of Practice for public consultation from 21 June 2017 to 21 July 2017 to all interested industry, consumer groups, and Government stakeholders.

Interested stakeholders can send all submissions and feedback to **submissions@datagovernanceaus.com.au** or alternatively through the DGA website.

We welcome your input during this period of consultation and look forward to receiving your views about the Draft Code of Practice and its core principles.

ABOUT THE DRAFT DGA CODE OF PRACTICE

The Code contains the following 9 core principles:

1. No-harm rule
2. Honesty & transparency
3. Fairness
4. Choice
5. Accuracy and access
6. Accountability
7. Stewardship
8. Security
9. Enforcement

ABOUT DGA

DGA is a not-for-profit association founded in 2016 in order to establish industry standards and benchmarks around the collection, use and management of data in Australia. DGA provides education, thought leadership and advocacy services to its members to promote and foster an understanding of how data can be used responsibly to drive innovation and competitive advantage while increasing consumer trust and complying with regulatory requirements.
The members of DGA come from a cross section of Australian industry and include major financial institutions, leading retailers, law firms, real estate corporations, aviation, and specialist data suppliers including technology, software and consulting service providers.

Table of contents

Preamble

Data Governance Australia ("DGA") sets leading industry standards and benchmarks for the responsible collection, use, management and disclosure of data.

The DGA Code of Practice ("Code") meets current industry needs for a flexible, future-proof approach to self-regulation.

By promoting a culture of best practice, the Code drives innovation by increasing consumer confidence and trust in the actions of members of the DGA ("Code Organisations").

It is a requirement of membership that Code Organisations ensure all of their interactions with data follows the Code principles of no-harm, honesty and transparency, choice, fairness, accuracy and access, accountability, stewardship and security ("Principles").

The Code supports compliant practices, but is not a guide to legal compliance and is not, and is not intended to become, a registered APP code under the Privacy Act 1988 (Cth).

As a condition of association with DGA, members are bound to follow both the Code and any Code Guidelines issued during the time of their membership. This Code and any Code Guidelines apply in addition to a Code Organisation's obligations at law and does not alter any such obligations. Where there is inconsistency between a Code Organisation's obligations at law and any Code Principle, the law will prevail.

The Code Principles have been developed to supplement rather than restate relevant regulatory provisions. Further detail on specific regulatory requirements can be found in the Code Guidelines and on the Code Resources page of the DGA website.

Application of the Code is overseen and administered by the Code Authority consisting of seven members – an independent Chair, three independent consumer representatives and three from industry.

The rules of the Code Authority are contained in the Code Authority Charter available in the Code section of the DGA website. The Code Authority is empowered to make determinations about Code compliance.

Golden rule

A Code Organisation must ensure that it acts consistent with the following Code Principles:

(a) No-harm;
(b) Honesty and transparency;
(c) Fairness;
(d) Choice for the subject individual (in relation to personal information about the individual);
(e) Accuracy and access;
(f) Stewardship;
(g) Security;
(h) Accountability; and
(i) Enforcement,

as set out in further detail in the Code.

This Code applies in addition to a Code Organisation's obligations at law and does not alter any such obligations. It is a fundamental condition for compliance with this Code that a Code Organisation complies with all applicable laws in relation to data and privacy.

Definitions

'harm'

Refers to an adverse impact on a subject individual that, having regard to all of the circumstances, is unreasonable and unjustified.

'unethical' / 'unethical use of data'

Refers to the use of personal information which:

(a) causes harm to an individual,
(b) is used for purposes that are not legitimate business purposes, or
(c) does not accord with reasonable community expectations.

'legitimate business purpose'

Refers to a lawful business purpose that is:

(a) consistent with the context in which consumers provide personal information; or
(b) considered by reasonable community expectations as appropriate,

taking in to consideration the nature and purpose of the business activities of a Code Organisation.

'personal information'

Has the same meaning as defined in the Privacy Act 1988 (Cth) and refers to "information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified individual, or an individual who is reasonably identifiable."

‘de-identified data’

Refers to data that:

(a) originally included, or constituted personal information, but which has been de-identified such that the data is no longer about an identifiable individual or an individual who is reasonably identifiable; or

(b) is about subject individuals but does not contain personal information or has been anonymised.

‘sensitive information’

Has the same meaning as defined in the Privacy Act 1988 (Cth) and refers to “information or an opinion (that is also personal information) about an individual’s:

- racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a trade union, sexual orientation or practices, or criminal record;
- health information about an individual;
- genetic information (that is not otherwise health information);
- biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or
- biometric templates.

‘APP and APPs’

Refer to the Australian Privacy Principles, which are contained in Schedule 1 of the Privacy Act 1988 (Cth).

Principle 1 - No-harm rule

1.1 Code Organisations must use best endeavours to ensure that they do not cause harm to a subject individual as a result of the collection, use, or disclosure of the subject individual's personal information.

1.2 Code Organisations must act with integrity and ensure that data is not used for a purpose that is reasonably considered to be unethical.

1.3 Code Organisations must not exploit, in circumstances where a Code Organisation is aware or should reasonably be aware of, the lack of knowledge or inexperience of a subject individual from which it collects data.

Principle 2 - Honesty and transparency

2.1 Code Organisations must act with honesty and transparency when collecting, using and disclosing data relating to subject individuals.

2.2 Code Organisations must ensure that their collection, use and disclosure of personal information is consistent and in accordance with:

(a) its privacy notification statement;
(b) its privacy policy; and
(c) reasonable community expectations.

2.3 Code Organisations must be clear and upfront about the facts and purpose of their collection, use and disclosure activities in relation to personal information, and ensure that their privacy policy and privacy notification statements are easily accessible, not misleading and up to date. Organisations must not knowingly or intentionally omit material information about their collection, use and disclosure activities.

2.4 Code Organisations are under a continuing notification obligation and must take reasonable steps to provide subject individuals with appropriate updates regarding any changes in its activities in relation to the collection, use and disclosure of data relating to subject individuals, including to ensure any required notice to, or consent by, the subject individuals remain current.

2.5 Code Organisations should provide clear and easily accessible mechanisms for individuals to enquire about the collection, use and disclosure of their personal information.

2.6 Code Organisations must take such steps (if any) as are, in the circumstances, reasonable to notify subject individuals at the point of collection, or as soon as is reasonably practicable, if the personal information provided by the subject individual:

(a) may be combined with other internal or external data sets (whether in an identified form or not) that the Code Organisation has access to; or

(b) enables de-identified data about that individual to be combined or associated with such personal information.

2.7 To the extent permitted by law, Code Organisations must, when requested by a subject individual, inform the subject individual of the identity or type of third parties to which it generally discloses personal information, where those third parties may use the personal information for its own purposes.

2.8 Code Organisations must not, without notice to, or the consent of, the subject individual, collect multiple data sets, which would not, on their own, constitute personal information but, when taken together, would constitute or contain personal information, unless the data sets are maintained subject to safeguards that prevent the re-identification of the subject individual within the data sets.

2.9 Code Organisations may only disclose personal information to a third party in accordance with the law and:

(a) where the Code Organisation has satisfied itself that the recipient is either another Code Organisation; or

(b) where the Code Organisation has used reasonable endeavours to ensure that the recipient agrees to comply with the principles set out in this Code.

In addition, a Code Organisation must not disclose personal information to a third party if it has reasonable grounds to suspect that the disclosed personal information will be used by the third party in an unlawful manner, or in a manner that may cause harm to the individual.

Principle 3 - Fairness

3.1 Code Organisations must only collect personal information from subject individuals for actual or anticipated legitimate business purposes (including those purposes which are contained in the privacy notification statement).

3.2 Code Organisations should consider the fairness of collecting, using and disclosing personal information, taking into account:

(a) the circumstances in which the personal information was collected;

(b) the appropriate period of time for which that personal information should be retained;

(c) the reasonable community expectations with respect to the use of personal information relating to them;
(d) subject to legal requirements, that personal information should be deleted or de-identified when it is no longer required for any other purpose for which the information may be used or disclosed; and
(e) the risk of harm to a subject individual.

3.3 Code Organisations must consider the evolving community expectations to the collection and use of data, when assessing whether a subject individual has a reasonable expectation of the particular use.

Principle 4 - Choice

4.1 Code Organisations must ensure that mechanisms, which provide choice for the collection and use of personal information, are easily accessible and understandable to subject individuals.

4.2 Code Organisations must not, unless required by law, re-identify external data sets that would reasonably likely contain sensitive information upon re-identification without the express consent of the subject individuals.

Principle 5 - Accuracy and access

5.1 Code Organisations must take reasonable steps to ensure that any data that they share is accurate and not misleading.

5.2 Code Organisations must, when requested, provide subject individuals with an easily accessible means to update personal information held about them in order to correct errors in, and ensure accuracy of, that personal information.

5.3 Code Organisations must only re-identify subject individuals within de-identified data sets in circumstances where the relevant Code Organisation has:

(a) a well-founded expectation that the subject individual to be re-identified is reasonably likely to be the correct individual;
(b) another legitimate business purpose for using such personal information; and
(c) complied with clauses 2.6 - 2.9.

5.4 Code Organisations should encourage the development and adoption of industry standards that support the effective implementation of the Code.

Principle 6 - Safety, security and de-identification

6.1 Code Organisations must design and organise their security (including encryption) in accordance with recognised industry standards as appropriate to the nature of the data it holds and the harm that may result from a security breach.

6.2 Code Organisations must nominate a specified individual or individuals tasked with responsibility for ensuring the security of the data it holds.

6.3 Code Organisations should seek to ensure that personal information is stored, shared or otherwise disclosed in encrypted or de-identified form and in accordance with recognised industry standards unless:

(a) it is not commercially reasonable;
(b) it is not technically feasible; or
(c) would make the proposed use impractical.

In addition, Code Organisations should use reasonable endeavours to ensure third party service providers comply with this principle.

6.4 Code Organisations should ensure that its de-identification processes remain robust by regularly:

(a) undertaking a review of the recognised industry standards of de-identification in the marketplace; and
(b) testing and updating its de-identification techniques with reference to recognised industry standards in the marketplace.

6.5 Where a Code Organisation collects or stores multiple data sets in de-identified form it must treat the data sets as personal information unless the Code Organisation applies appropriate security measures and de-identification techniques (consistent with recognised industry standards) to ensure that the data sets cannot reasonably be combined or matched to re-identify subject individuals.

Principle 7 - Stewardship

7.1 Code Organisations should ensure any contractors and/or employees responsible for data storage and data security are adequately trained and understand the obligations of their role and under this Code.

7.2 Code Organisations must appoint a relevant officer responsible for compliance with this Code.

7.3 Code Organisations must develop and implement appropriate internal processes that support and ensure compliance with this Code.

7.4 Code Organisations should ensure that its employees receive adequate training regarding appropriate data handling practices to promote organisation-wide compliance with this Code.

Principle 8 - Accountability

8.1 Code Organisations must take steps to create and maintain a register or registers of the classes or categories of personal information which they collect, use and disclose, including:

(a) how the personal information is collected, used and disclosed; and
(b) which third parties the personal information is disclosed to.

8.2 Code Organisations must ensure the information of the person appointed for ensuring compliance with this Code is publicly available and easily accessible.

8.3 Code Organisations must have a clear and publicly available statement and/or use the DGA Trust Mark to demonstrate commitment to and compliance with this Code.

Principle 9 - Enforcement

9.1 As a condition of membership Code Organisations must comply with this Code and the Code Guidelines issued and enforced from time to time during the term of the Code Organisation's membership of the DGA.

9.2 Code Organisations must agree to the enforcement of this Code by the Code Authority pursuant to the Code Authority Charter as a condition of DGA membership.

DATA GOVERNANCE AUSTRALIA

MELBOURNE

Level 17,
600 Bourke Street,
Melbourne,
VIC 3000

SYDNEY

Level 6,
50 Carrington Street,
Sydney,
NSW 2000

www.datagovernanceaus.com.au

contact@datagovernance.com.au