

FSDf SPATIAL INFORMATION MANAGEMENT POLICIES – PRIVACY

Objective: Protecting individual's information within the Foundation Spatial Data Framework.

This document is presented by ANZLIC – the Spatial Information Council, representing the Australian and New Zealand Governments, and the governments of the States and Territories of Australia.

*The Australian and New Zealand Foundation Spatial Data Framework:
FSDf Spatial Information Management Policies - Privacy.*

About this document

This document has been published by the Department of Communications on behalf of ANZLIC—the Spatial Information Council. ANZLIC is an intergovernmental council that comprises representatives from the Australian, state and territory governments and the New Zealand Government. The ANZLIC Secretariat is currently provided by the department.

Digital versions of this publication are also available on the ANZLIC website at www.anzlic.org.au/FSDf.

Copyright notice



© The Commonwealth of Australia (Department of Communications) 2014.

With the exception of the ANZLIC logo, any material protected by a trade mark and where otherwise noted; this work is licensed under a Creative Commons Attribution 3.0 Australia licence (<http://creativecommons.org/licenses/by/3.0/au/>).

Contact details

For information about ANZLIC—the Spatial Information Council or if you would like more information on this document, please contact:

ANZLIC Secretariat
Department of Communications
GPO Box 2154
Canberra ACT 2601
Phone: 02 6271 1493 (international +61 2 6271 1493)
Email: spatial@communications.gov.au
Web: www.anzlic.org.au

Table of Contents

Document Versioning	3
FSDF Privacy Policy.....	4
Introduction	4
Purpose	4
Policy Reform - Australian Privacy Principles	4
Privacy Policy Governance	4
Roles and Responsibilities.....	5
Annex:	5
Annex A – Australian Privacy Principles (from 12 March 2014)	1

Document Versioning

Date	Version No.	Description	Author
18 Feb 2014	0.1	First draft	Spatial Policy Branch (SPB)
17 Mar 2014	0.2	Contact Officer comments (VIC)	SPB

FSDf Privacy Policy

Introduction

1. This document defines the information privacy arrangements that have been established to support the implementation of the Australian and New Zealand Foundation Spatial Data Framework (FSDf). The applicable overarching policy is the Commonwealth Privacy Act 1988. Where equivalent New Zealand Government privacy policy applies, acknowledgement will be made in future iterations of this document.
2. The FSDf is a federated project across the Commonwealth governments of Australia and New Zealand and the governments of the States and Territories of Australia. During the process of information collection and aggregation, organisations must ensure the protection of personal information according to the laws governing their particular jurisdiction.

Purpose

3. The purpose of this document is to describe the framework for applying privacy policy within the FSDf. The policy relates to the protection of an individual's personal information, information that identifies a person or could reasonably identify a person.

Policy Reform - Australian Privacy Principles

4. The Commonwealth Privacy Act 1988 has been amended and with effect 12 March 2014, all Australian businesses and Commonwealth (and ACT government) agencies will be subject to a new set of Australian Privacy Principles listed at annex A.

Privacy Policy Governance

5. The major stakeholders in the FSDf, the Australian state, territory and Commonwealth and New Zealand governments, have discrete privacy legislation and subordinate policies covering their jurisdictional agencies/organisations. The FSDf, which aggregates data from all jurisdictions, will need to reconcile the aggregation process and policies in order to achieve a homogeneous national dataset(s) for each FSDf theme.

6. The currency and application of this policy is the responsibility of the FSDf secretariat in coordination with the sponsors/custodians of the FSDf themes/National Spatial Datasets. Where significant changes occur to Privacy policy covering either the source or aggregated data, a review and response is required within the management processes under the FSDf Governance Model.

Roles and Responsibilities

7. FSDf Secretariat – monitoring the legislation, rules and guidance relating to Privacy and management of the FSDf Privacy policy and implementation.
8. Theme Sponsors – guidance on the application of Privacy Policy within the FSDf.
9. National Dataset Custodian – management of privacy for data in the National Spatial Dataset aggregated from multiple sources.
10. Jurisdictional agencies/organisations – application of privacy of policy in accordance with the legislation and requirements of their jurisdiction.

Annex:

- A. Australian Privacy Principles (from 12 March 2014)

Annex A – Australian Privacy Principles (from 12 March 2014)

APP 1 — Open and transparent management of personal information

Ensures that APP entities manage personal information in an open and transparent way. This includes having a clearly expressed and up to date APP privacy policy.

APP 2 — Anonymity and pseudonymity

Requires APP entities to give individuals the option of not identifying themselves, or of using a pseudonym. Limited exceptions apply.

APP 3 — Collection of solicited personal information

Outlines when an APP entity can collect personal information that is solicited. It applies higher standards to the collection of 'sensitive' information.

APP 4 — Dealing with unsolicited personal information

Outlines how APP entities must deal with unsolicited personal information.

APP 5 — Notification of the collection of personal information

Outlines when and in what circumstances an APP entity that collects personal information must notify an individual of certain matters.

APP 6 — Use or disclosure of personal information

Outlines the circumstances in which an APP entity may use or disclose personal information that it holds.

APP 7 — Direct marketing

An organisation may only use or disclose personal information for direct marketing purposes if certain conditions are met.

APP 8 — Cross-border disclosure of personal information

Outlines the steps an APP entity must take to protect personal information before it is disclosed overseas.

APP 9 — Adoption, use or disclosure of government related identifiers

Outlines the limited circumstances when an organisation may adopt a government related identifier of an individual as its own identifier, or use or disclose a government related identifier of an individual.

APP 10 — Quality of personal information

An APP entity must take reasonable steps to ensure the personal information it collects is accurate, up to date and complete. An entity must also take reasonable steps to ensure the personal information it uses or discloses is accurate, up to date, complete and relevant, having regard to the purpose of the use or disclosure.

APP 11 — Security of personal information

An APP entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure. An entity has obligations to destroy or de-identify personal information in certain circumstances.

APP 12 — Access to personal information

Outlines an APP entity's obligations when an individual requests to be given access to personal information held about them by the entity. This includes a requirement to provide access unless a specific exception applies.

APP 13 — Correction of personal information

Outlines an APP entity's obligations in relation to correcting the personal information it holds about individuals.

These principles apply to:

Private sector organisations, Australian Government, ACT Government and Norfolk Island agencies covered by the *Privacy Act 1988*