

PRIVACY POLICY

The Privacy Act (Cth) 1998 ("Privacy Act") is intended to establish a comprehensive national scheme for the collection, holding, use, correction, disclosure and transfer of personal information by organisations in the private sector. This gives individuals the right to know what information an organisation holds about them and a right to correct that information if it is wrong.

This policy is to ensure Strategem complies with the Privacy Act established for the handling of personal information by organisations in the private sector. Strategem will ensure that it complies with the ten National Privacy Principles (NPPs) set out by the Privacy Act. The NPPs regulate the way Strategem can collect, use, disclose, amend and pass on personal information.

Responsibility and Authority

All Managers and Staff

- Ensure compliance with the policy

Privacy Compliance Officer

- Receives complaints from an individual regarding an alleged breach of privacy by Strategem
- Investigates and resolves the complaint internally through mediation with the individual
- Strategem's Privacy Officer is Julie Stratford

Principle 1: Collection of information

Personal information will only be collected to the extent necessary by lawful and fair means and not in an unreasonably intrusive way for one or more of Strategem's functions or activities.

At the time of collection (or as soon as practicable afterwards) Strategem will take reasonable steps to ensure that the individual is told:

- how he or she may contact Strategem
- that they can access the information;
- why the information is collected;
- the disclosure practices of Strategem
- any law that requires the particular information to be collected and the consequences (if any) for the individual if the information is not provided; and
- the main consequences (if any) for the individual if all or part of the information is not provided.

Principle 2: Use of information

Strategem will use or disclose personal information for the primary purpose for which it was collected.

Strategem will use personal information for another purpose (secondary purpose) if:

- 1) the individual has consented; or
- 2) the secondary purpose is related to the primary purpose and the individual would reasonably expect Strategem to use or disclose the information for the secondary purpose. If the personal information is sensitive information, the secondary purpose must be directly related to the primary purpose of collection; or
- 3) if the information is not sensitive information, Strategem will use the information for the secondary purpose of direct marketing if:

- (i) it is impracticable to seek the individual's consent before the particular use; and
- (ii) there is no charge for implementing an individual's request to Strategem not to receive direct marketing; and
- (iii) the individual has not made a request to Strategem not to receive direct marketing; and
- (iv) in each direct marketing communication with the individual, Strategem notifies the individual that they may elect not to receive any further direct marketing communications; and
- (v) each written direct marketing communication with the individual by Strategem sets out Strategem's business address, telephone number and email address at which Strategem can be contacted directly; or

- 4) Strategem reasonably believes that the use or disclosure is necessary to lessen or prevent a serious and imminent threat to an individual's life, health or safety or a serious threat to public health or public safety; or
- 5) Strategem has reason to suspect that unlawful activity has been, is being or may be engaged in, and uses or discloses the personal information as a necessary part of its investigation of the matter or in reporting its concerns to relevant authorities or persons; or

PRIVACY POLICY

- 6) The use or disclosure is required or authorised by or under law; or
- 7) Strategem reasonably believes that the use or disclosure is reasonably necessary for one or more of the following by or on behalf of an enforcement body:
- (a) The prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law; or
 - (b) the enforcement of laws relating to the confiscation of the proceeds of crime; or
 - (c) the protection of the public revenue; or
 - (d) the prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct; or
 - (e) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal.

Any personal information used or disclosed for any of the reasons in this paragraph 7, must be recorded in writing

Principle 3: Data quality

Strategem will take reasonable steps to ensure that personal information it collects uses or discloses is accurate, complete and up to date.

Principle 4: Data security

Strategem will take reasonable steps to protect personal information it holds from misuse and loss and from unauthorised access, modification or disclosure. Strategem will also take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose for which the information may be used or disclosed under Principle 2.

Principle 5: Openness

Strategem will have clearly expressed policies on its management of personal information and these will continue to be readily available. On request from an individual, Strategem will

take all reasonable steps to let the individual know, generally, what sort of personal information it holds, for what purposes, and how it collects, uses, and discloses that information. Strategem otherwise complies with the NPPs under the Privacy Act.

Principle 6: Access and correction

6.1 Where Strategem holds personal information about an individual, it will provide the individual with access to the information on request, except to the extent that:

- a) in the case of personal information other than health information - providing access would pose a serious and imminent threat to the life or health of any individual; or
- b) in the case of health information – providing access would pose a serious threat to the life or health of any individual; or
- c) Providing access would have an unreasonable impact upon the privacy of other individuals; or
- d) The request for access is frivolous or vexatious; or
- e) The information relates to existing or anticipated legal proceedings between Strategem and the individual, and the information would not be accessible by the process of discovery in those proceedings; or
- f) providing access would reveal the intentions of Strategem in relation to negotiations with the individual in such a way as to prejudice those negotiations; or
- g) Providing access would be unlawful; or
- h) Denying access is required or authorised by law; or
- i) Providing access would be likely to prejudice an investigation of possible unlawful activity; or
- j) Providing access would be likely to prejudice:
 - (i) the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law; or
 - (ii) the enforcement of laws relating to the confiscation of the proceeds of crime;
 - (iii) the protection of the public revenue;
 - (iv) the prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct; or
 - (v) preparation for, or conduct of, proceedings before any court or tribunal, or implementation of its

PRIVACY POLICY

orders; by or on behalf of an enforcement agency; or
 k) an enforcement body performing a lawful security function asks Strategem not to provide access to the information on the basis that providing access would be likely to cause damage to the security of Australia.

Where providing access would reveal evaluative information generated within Strategem in connection with a commercially sensitive decision-making process, Strategem may give the individual an explanation for the decision, rather than direct access to the information.

Where Strategem not required to provide the individual with access to the information for any reason set out in 6.1, Strategem will, if reasonable, consider whether the use of mutually agreed intermediaries would allow sufficient access to meet the needs of both parties.

6.4 If Strategem levies charges for providing access to personal information, those charges:

- (a) will not be excessive; and
- (b) will not apply to lodging a request for access.

6.5 If Strategem holds personal information about an individual and the individual is able to establish that the information is not accurate, complete and up-to-date, Strategem will take reasonable steps to correct the information so that it is accurate, complete and up-to-date.

6.6 If the individual and Strategem disagree about whether the information is accurate, complete and up-to-date, and the individual asks Strategem to associate with the information a statement claiming that the information is not accurate, complete or up-to-date, Strategem will take reasonable steps to do so.

6.7 Strategem will provide reasons for denial of access or a refusal to correct personal information.

Principle 7: Identifiers

Strategem will not adopt as its own identifier an identifier that has been assigned by a government agency (or by the government's

agent or contractor). Examples are an individual's medicare or tax file number. Strategem will not use or disclose an identifier assigned to an individual by a government agency except where paragraphs 2(4) to 2(7) of Principle 2 above apply, or it is necessary for Strategem to fulfil its obligations to the agency. An individual's name or ABN is not an identifier.

Principle 8: Anonymity

Whenever it is lawful and practicable, individuals will have the option of not identifying themselves when entering transactions with Strategem.

Principle 9: Transborder data flows

Strategem will not transfer personal data outside Australia unless:

- (a) Strategem reasonably believes that the recipient of the information is subject to a law, binding scheme or contract which effectively upholds principles for fair information handling that are substantially similar to the NPPs; or
- (b) the individual concerned consents to the transfer; or
- (c) the transfer is necessary for the performance of a contract between the individual concerned and Strategem or for the implementation of pre-contractual measures taken in response to the individual's request; or
- (d) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual concerned between Strategem and a third party; or
- (e) the transfer is for the benefit of the individual concerned; and
- (i) it is not practicable to obtain the consent of the individual to that transfer; and
- (ii) if it were practicable to obtain such consent, the individual would be likely to give it; or
- (f) Strategem has taken reasonable steps to ensure that the information which it has transferred will not be held, used or disclosed by the recipient of the information inconsistently with these rules.

Principle 10: Sensitive Information

Strategem will not collect sensitive information about an individual unless:

- (a) the individual has consented; or
- (b) the collection is required by law; or
- (c) the collection is necessary to prevent or lessen a serious and imminent threat to the

PRIVACY POLICY

life or health of any individual, where the individual whom the information concerns:

(i) is physically or legally incapable of giving consent; or

(ii) physically cannot communicate consent to the collection; or

(d) the collection is necessary for the establishment, exercise or defence of a legal or equitable claim.

personal information means information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

sensitive information means:

(a) information or an opinion about an individual's:

(i) racial or ethnic origin; or

(ii) political opinions; or

(iii) membership of a political association; or

(iv) religious beliefs or affiliations; or

(v) philosophical beliefs; or

(vi) membership of a professional or trade association; or

(vii) membership of a trade union; or

(viii) sexual preferences or practices; or

(ix) criminal record;

that is also personal information; or

(b) health information about an individual; or

(c) genetic information about an individual that is not otherwise health information.

EXEMPTION

There is an exemption in the Privacy Act regarding information relating to a current or former employee. The Privacy Act does not apply to an act done or practice engaged in by Strategem in relation to:

- A current or former employment relationship between Strategem and the individual; and
- An employee record held by Strategem relating to the individual (includes personal information relating to the employment relationship and may include information, such as recruitment/termination information, terms and conditions of employment, health and banking details).

This exemption does not apply to applicants who are unsuccessful in securing a role at Strategem. In those cases, Strategem will take all the necessary steps to ensure proper collection, use, storage, disclosure of and access to information in accordance with the Privacy Act and other applicable laws.

Procedure for making a complaint

A person may make a complaint if they feel their personal information has been handled inappropriately by a private sector organisation in breach of Strategem's privacy obligations under the Privacy Act.

In the first instance, complaints must be directed to Strategem's Privacy Officer in writing. Strategem will investigate the complaint and prepare a response to the complainant in writing within a reasonable period of time.

If the complainant is not satisfied with Strategem's response or the manner in which Strategem has dealt with the complaint, the individual may make a formal complaint to the Office of the Federal Privacy Commissioner ("OFPC"). The OFPC will provide Strategem with the opportunity to respond to the complaint. Following its enquiries, if the OFPC decides that there is insufficient evidence to support the complaint, the OFPC may dismiss the complaint. Alternatively, if the OFPC believes there is enough evidence to support the complaint, it will try to conciliate the matter.

If conciliation does not resolve the complaint, depending on the circumstances, the Privacy Commissioner may either close the file or make a determination. A determination could include a requirement that Strategem issue an apology, improve practices to reduce likelihood of a breach of the Privacy Act, or compensation to be paid to the complainant.

If the OFPC closes the file, the complainant may apply to the Federal Court or the Federal Magistrates Court by way of appeal. Either party may also appeal to the Administrative Appeal Tribunal for a review of any compensation amount ordered by the Privacy Commissioner.

Strategem may amend and vary this policy from time to time.

Contact Details

Privacy Officer: Julie Stratford

Address: 35 Mundy Street Bendigo

Telephone: 03 5445 4777

Facsimile: 03 5441 5264

e-mail: julie.stratford@strategem.com.au