PERTH CONVENTION BUREAU

PRIVACY STATEMENT

The Perth Convention Bureau (PCB) is a not for profit organisation with the primary role of marketing Western Australia as a destination for meetings, incentive travel, conventions and exhibitions.

We understand the need to protect personal information from misuse, and respect everyone's right to privacy, therefore we have procedures in place to protect your personal information.

Our Privacy Policy, which complies with the National Privacy Principles, covers the collection, use, storage and disclosure of personal information. We have a Privacy Officer on the team who is responsible for constantly monitoring all aspects of information usage to ensure your information is protected.

We strive to maintain an open and accountable policy on the privacy of personal information and our Privacy Officer is available to discuss this policy and any queries you might have.

For further details on PCB's privacy policy contact:

Paul Beeson
Perth Convention Bureau
Telephone: +61 (0) 8 9218 2900
Facsimile: +61 (0) 8 9218 2910

PRIVACY POLICY – (NPP5.1)

1. Purpose

The Perth Convention Bureau (PCB) is committed to the protection of personal privacy and as such has adopted a set of privacy principles.

PCB understands you care how your personal information is handled and will comply with the Australian National Privacy Principles of the Privacy Act (Private Sector) Amendment 2000.

2. Policy

This policy sets out the principles that PCB has adopted in order to protect personal information about individuals, covering both external individuals and internal staff. These principles deal with collection, use and disclosure of personal information as well as access to information and intrusion issues. These Privacy Protection Principles are;

2.1 Collection of Personal Information

PCB will only collect personal information that is necessary for one or more of its legitimate functions or activities.

PCB will only collect information by lawful and fair means not in an unreasonably intrusive way.

At or before the time PCB collects personal information from the subject of the information (or, if that is not practical, as soon as practicable thereafter), PCB will take reasonable steps to ensure that the subject of the information is aware of:

(a) PCB's identity and how to contact us;

(b) the fact that he or she is able to gain access to the information;

(c) the purpose for which the information is collected;

(d) to whom (or the types of individuals or organisations to which) PCB discloses information of this kind.

Where it is reasonable and practicable to do so, PCB will take reasonable steps to ensure that the subject of the information is or has been made aware of the matters listed from (a) to (d) above.

2.2 Use
PCB primarily collects data on individuals and organisations that have the potential to meet in Western Australia for the purpose of accelerating the growth of the convention and incentive industry here.

The Bureau also facilitates contact between local suppliers and meeting organisers by providing information on confirmed meetings and events to its members and providing meeting planners with contacts to supply goods and services to stage their events here.

For the benefit of its members, PCB also organises regular networking and educational functions to which it issues invitations.

Both meeting planners and members also receive regular communication to brief them on industry issues and trends, new product and destination information.

Data on meetings and events held here is also collected for statistical purposes to evaluate the size and scope of the meeting industry in Western Australia.

PCB will only use personal information that is collected for a secondary purpose if it relates to the primary purpose of collection and a reasonable expectation to this use is present.

2.3 Disclosure
PCB will only disclose personal information for a secondary purpose if;

(a)
- (i) The secondary purpose is related to the primary purpose of collection; and
- (ii) The subject of the information would reasonably expect PCB to disclose the information for the secondary purpose; and
- (iii) The disclosure is made in the performance of a person's duties as an employee, agent or contractor or PCB

(b) the individual has consented to the disclosure; or

(c) the third party is an agent or contractor of PCB who is required to keep the information confidential and to use it only for the purpose for which it was disclosed.

2.4 Data Quality
PCB will take reasonable steps to make sure the personal information it collects, uses or discloses is accurate, complete and up- to- date.

2.5 Data Security
PCB will take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure.

PCB will take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose.

2.6 Openness
PCB will have clearly expressed policies on its management of personal information and these will continue to be readily available.

Upon request PCB will take reasonable steps to let individuals know, generally, what sort of personal information it holds, for what purposes, and how it collects, uses and discloses that information.

2.7 Access and Correction
Where PCB holds personal information about an individual, it will provide the individual with access to the information upon written request, in a form or manner suitable to the individuals reasonable needs, except to the extent that:

(a) providing access would have an unreasonable impact on the privacy of other individuals; or

(b) the information relates to existing legal dispute resolution proceedings PCB and the individual, and the information would not be accessible by the process of discovery in those proceedings; or

(c) providing access would reveal the intentions of PCB in relation to negotiations with the individual in such a way as to prejudice those negotiations.

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

If PCB has given an individual such an explanation and the individual believes that direct access to the evaluative information is necessary to provide a reasonable explanation of the reasons for the decision, PCB will, at the request of the individual, undertake a review of the decision. The review will be undertaken by personnel other than the original decision maker.

Wherever direct access by the individual is impractical or inappropriate, PCB and the individual should consider whether the use of mutually agreed intermediaries would allow sufficient access to meet the needs of both parties.

If PCB levies charges for providing access to the information, those charges;

(a) will not be excessive

(b) will not apply to lodging a request for access

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

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

PCB will provide reasons for denial of access or correction.

2.8 Identifiers
PCB adopts its own identifiers for all contacts.

2.9 Anonymity
Whenever it is lawful and practicable, individuals will have the option of not identifying themselves when dealing with PCB.

2.10 Transborder Data Flows
PCB will not transfer personal information outside of Australia unless;

(a) PCB reasonably believes that the recipient of the information is subject to statute, binding scheme or contract which effectively upholds principles for the fair information handling that are substantially similar to these rules; 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 PCB, or for the implementation of pre- contractual measures taken in respect 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 PCB 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 subject of the information to the transfer; and

  (ii) if it were practicable to obtain such consent, the subject of the information would give it; or

(f) PCB has taken reasonable steps to ensure that the information which it has transferred will not be collected, held, used or disclosed by the recipient of the information inconsistently with these rules.

2.11 Sensitive Information
PCB will not collect personal information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, or sexual activity.

2.12 Mandatory data breach notification laws
The Privacy Amendment (Notifiable Data Breaches) Act 2017made its way through both houses of Parliament with bipartisan support and received Royal Asset on 22 February 2017. This will mean that, from 23 February 2018 (or earlier if a date is fixed by

proclamation), the Privacy Act 1988 (Cth) will include a mandatory data breach notification scheme.

What you need to do

Organisations and Federal agencies subject to the Privacy Act (APP Entities) should take steps now to ensure that their practices and procedures will enable them to meet the new obligations to which they will be subject under the amended legislation.

The mandatory data breach notification scheme

The mandatory data breach notification scheme being introduced will require APP Entities to promptly notify the Office of the Australian Information Commissioner (OAIC) and any potentially affected individuals of an "eligible data breach".

The underlying purpose of the scheme is to ensure that individuals can take remedial steps in the event that their personal information is compromised.

When does the notification obligation arise?

The amended Privacy Act will require APP Entities to provide notice as soon as practicable to the OAIC and affected individuals where there are reasonable grounds to believe that an "eligible data breach" has occurred (unless an exception applies). Relevantly:

- a data breach will arise where there has been unauthorised access to, or unauthorised disclosure of, personal information about one or more individuals, or where such information is lost in circumstances that are likely to give rise to unauthorised access or unauthorised disclosure (for example, leaving the information on the bus);
- an eligible data breach will arise where a reasonable person would conclude that there is a likely risk of serious harm to any of the affected individuals as a result of the unauthorised access or unauthorised disclosure;
- serious harm, while undefined, is likely to include serious physical, psychological, emotional, economic and financial harm, as well as serious harm to reputation; and
- serious harm will be likely if such harm is "more probable than not" having regard to a list of relevant matters to be included in Part IIIC. The matters include the sensitivity of the information, any security measures taken (such as encryption) and how easily those security measures could be overcome (for example, if the encryption key has also been accessed).

This notification obligation will involve at least a two-step process. First, the APP Entity must prepare a statement containing certain prescribed information about the data breach and provide it to the OAIC. The APP Entity must then take steps to notify the affected individuals. The actual steps required will depend on the circumstances, but will usually include sending the statement to the individual via the usual means of communication between the APP Entity and individual.

If an APP Entity only has reasonable grounds to suspect that an eligible data breach has occurred, the notification obligation will not arise, However, the APP Entity will be required by the new legislation to complete a "reasonable and expeditious" assessment

into the relevant circumstances within 30 days. Importantly, shutting one's eyes will not allow APP Entities to avoid the requirements of the Privacy Act.

Exceptions to the data breach notification requirement

Various exemptions to the notification requirement will be included in the amended legislation.

Perhaps the most interesting exception is that a notification will not need to be given if the APP Entity takes remedial action before any serious harm is caused by the breach.

This exemption demonstrates the value of early detection and action. Importantly, the ability of a company to detect a data breach at the first available opportunity and take action in respect of it will be a function of the organisation's preparedness for such an occurrence.

In order to be properly prepared, it is likely that a prudent organisation will have in place detailed policies and procedures which outline the steps that are to be taken in response to a serious data breach, regardless of whether that breach has occurred as a result of inadvertence on the part of the organisation and its employees (eg. as a result of personal information being lost) or following a co-ordinated attack by hackers.

Penalties

A failure to comply with the notification obligations will fall under the Privacy Act's existing enforcement and civil penalty framework. Accordingly, APP Entities may be subject to anything from investigations to, in the case of serious or repeated non-compliance, substantial civil penalties.

What should you do

APP Entities have less than 12 months to prepare for the introduction of the mandatory data breach notification scheme. That time should be used wisely by APP Entities to:

- audit their current information security processes and procedures to ensure they are adequate (prevention will soon be much more palatable than the cure); and
- prepare a data breach response plan (or update their current plan) so as to enable the APP Entity to respond quickly, efficiently and lawfully to an actual or suspected data breach.

The OAIC currently operates a voluntary data breach notification scheme and has published various resources to assist APP Entities with their handling of data breaches. Much of that guidance will assist APP Entities in ensuring that they comply with the mandatory data breach notification scheme and it is expected that the OAIC will release new or updated guidance over the coming months.

However, further steps are likely to be necessary in order to ensure that your organisation understands the impact of the scheme and to make the necessary preparations for its introduction.

3.