PRIVACY POLICY

April 2017

Energy Action Limited
ABN 90 137 363 636

Contents

1.0 Introduction 3
2.0 Collection of Information 3
3.0 Method of Collection 4
4.0 Use and Disclosure of Personal Information 4
5.0 Cross border disclosure of personal information 5
6.0 Shareholders 5
7.0 Management of Personal Information 6
8.0 Accessing and correcting your Personal Information 6
9.0 Data Security 7
10.0 Authorities and Responsibilities 8
11.0 Complaints 8

1.0 Introduction

Energy Action Limited (***Energy Action***) and its subsidiaries (together Energy Action) is committed to ensuring the privacy and security of the personal information we collect and hold about individuals. Energy Action complies with all requirements of the Privacy Act 1988 (Cth) (***Privacy Act***) and the and the Australian Privacy Principles (***Principles***) when it deals with personal information. This Privacy Policy has been adopted by Energy Action in accordance with Australian Privacy Principle 1.3, and is intended to provide you with information on how we manage the personal information we hold about you. This policy applies to all individuals from whom Energy Action collects personal information in the course of its dealings with them.

We respect the privacy of all our clients, shareholders and visitors of our website. We understand that you expect privacy in your transactions with us. We will keep your information secure and handle it strictly in accordance with the law.

This Privacy Policy will be revised as and when circumstances change.

2.0 Collection of Information

Energy Action collects certain personal information about individuals in order to understand and meet the needs of clients and provide the products and services they require, and for various other purposes described in this Privacy Policy. Energy Action will only collect your personal information if it is reasonably necessary for its business activities.2.1 Types of Information Collected

The type of personal information Energy Action collects and holds about you will depend on the circumstances of collection, including whether we collect the information form you as a client, supplier, stakeholder, job applicant or in some other capacityTherefore depending on the type of contact you have with us, we may collect and holdincludes:

- contact details (such as your name, address, telephone number or email);
- personal details (such as your date of birth, gender or occupation);
- financial information (such as your bank account details or details relevant to your investment in Energy Action);
- tax file number (or the exemption reason or country of residence);
- information about entities in which you have an interest (either as an investor or office holder)
- if you are a client – details of your energy retailer, copies of invoices and metering data
- etails of your interactions and transactions with us, including records of any contact we have with you by telephone or email.

We do not collect sensitive information about you. 'Sensitive information' means information or an opinion about your race, ethnic origin, political opinions, religious or philosophical beliefs, sexual preferences, criminal record or health and genetic information.

3.0 How we collect your personal information

Energy Action collects personal information directly from you in a variety of ways, including from you directly (including when you interact with us in writing, electronically or via telephone), when you visit our website, when you participate in our events, trade show or other function attended by Energy Action. In certain situations where it is unreasonable or impractical to collect personal information from you, we may collect personal information about you from someone else, including public sources (such as telephone listings), our related companies, your organisation, your authorised representatives (if you have authorised us to collect information from them), information service providers and external service providers. At all times, the collection of this information is obtained by lawful means in a manner that respects your privacy.4.0 How do we use your personal information?

Your privacy is respected and we do not sell, rent or trade your personal information. If we collect your personal information, we will only use or disclose your personal information for that purpose to effectively conduct our business, unless you consent to Energy Action using the information for another purpose, or unless we are required or authorised by law to use the information for another purpose.

In general, Energy Action may use or disclose personal information for the following purposes:

- to provide products and services to clients;
- to understand our clients and what products and services best suit their needs (including market research purposes);
- to service shareholders;
- to respond to queries, complaints or to provide you with our general client services;
- to verify your identity and personal information;
- to maintain and update our records;
- to communicate with contractors and suppliers;
- to provide ongoing information about our products and services to people that we believe may be interested;
- to help manage and enhance our products and services, including by surveying clients on their future needs;
- to consider applications for employment;
- to facilitate any purchase or potential purchase of an interest in our business;
- to protect our lawful interests; and
- to comply with legal obligations, for example, Energy Action may disclose your personal information to comply with a court order demanding the disclosure or the information or with a request by a government agency for the product of records pursuant to taxation or social security laws.

If you are the contact person for a customer or supplier, we may also use your personal information such as your name to manage our relationship with your organisation.We may also use your personal information to promote and market products and services to you. This is to keep you informed of products, services and special offers and may continue after you cease to acquire services from us. We will only use your information for this purpose in circumstances permitted by law (including by the Privacy Act, Spam Act 2003 and the Do Not Call Register Act 2006).

If you do not wish us to contact you to promote and market products, services and special offers, or if you have subscribed to any of our newsletters or subscriptions and no longer wish to receive such communications, please email marketing@energyaction.com.au.

Depending on the product or service or issue concerned, we may disclose personal information to:

- service providers and specialist advisers who have been contracted to provide administrative, financial, research or other services, including mail houses, share registry and information technology support;
- companies within the Energy Action group;
- insurers, credit providers, courts, tribunals and regulatory authorities (including the
- Australian Tax Office) as required or authorised by law; or
- your authorised representatives (if you have authorised us to disclose the information to them).

5.0 Cross border disclosure of personal information

Energy Action will generally not send information overseas.

However, in rare circumstances, and under strict control to ensure there is no breach of the Principles, Energy Action may authorise access to personal information by restricted persons in an overseas location. Energy Action will comply with all applicable laws if it does this. [Overseas countries might include, but are not limited to, [*] and [*].]

6.0 Shareholders

If you are a shareholder of Energy Action, you may provide us with your tax file number, which we will keep securely on the relevant share register. In accordance with Australian tax laws, we may provide certain advice to the Australian Tax Office, including dividend information.

Section 173 of the Corporations Act *2001* requires Energy Action to grant access on request to their share register.

The share register sets out all shareholders' names, addresses and share holdings. We may provide information from the share register to meet specific requests such as identifying the top 100 shareholders. Shareholder information is not disclosed for purposes other than those for which we are required or authorised by law to disclose.

Energy Action may disclose your personal information to your stockbroker, accountant, a family member or other person who you have authorised to be contacted on your behalf. In those circumstances, you will be required to identify that party as your authorised agent.

7.0 Management of Personal Information

Energy Action has implemented appropriate technological and organisational measures to assist us in ensuring the protection of your personal information.

We expect our employees and contractors who handle personal information to comply with the Privacy Act and will take appropriate action in response to breaches of the obligations imposed by the Principles. Although we seek to engage external service providers who also comply with these requirements, we do not accept responsibility for the misuse of personal information by these third parties.

8.0 Accessing and correcting your Personal Information

Under the Principles, you usually have the right:

- to obtain a copy of any personal information which Energy Action holds about you; and
- to request that we correct information we hold about you.

You may request to access your personal information, or request a correction be made to that information by contacting us by:

Post: Energy Action Limited - Marketing
Level 5, 56 Station Street
Parramatta NSW 2150

Telephone: 1300 553 551 or 02 9633 6400

Fax: 02 9475 0954 (Attn: Marketing)

Email: marketing@energyaction.com.au

Depending upon the personal information you seek, or the correction you request to be made to your personal information, you may be asked:

- to complete an Information Request Form;
- to verify your identity in writing; and/or
- to ensure the integrity of the information, to provide evidence in support of the correction you are requesting we make to your information.

Energy Action will endeavour to provide you with the personal information you request access to within a reasonable timeframe and in any reasonable manner requested by you.

Please note that in circumstances prescribed by the Privacy Act, you may be refused access to your personal information (for example, if providing access would be unlawful or would have an unreasonable impact upon the privacy of other individuals). Where a written request by you to access information is refused, we will generally give you a written response to your request setting out the reasons for the refusal and the mechanisms available to you to complain about the refusal.

Energy Action will consider any request by you to change or correct your personal information and respond within a

reasonable timeframe.

Where a written request by you to correct your personal information is refused, we will generally provide you with a written response to your request setting out the reasons for the refusal and the mechanisms available to you to complain about the refusal.

We will take reasonable steps in the circumstances to ensure your personal information:

- collected by us is accurate, complete and up to date; and
- used or disclosed by us is accurate, up to date, complete and relevant,

however, we rely on you to notify us of any changes to your personal information.

9.0 Data Security

Energy Action will take reasonable steps to protect your personal information from misuse, interference, loss, unauthorised access, modification or disclosure. We use technologies and processes such as [access control procedures, network firewalls, intrusion detection systems, virus scanning tools, encryption and physical security] to protect your privacy. We review and update our security measures as appropriate.

Other security measures may include, depending on the circumstances:

- management of access privileges, to ensure that only those who really need it can see your personal information;
- secure work environments and workflow systems that prevent unauthorised access and copying of your personal information; and
- ensuring that our external service providers maintain appropriate security measures.

Energy Action will take reasonable steps to destroy or permanently de-identify any of your information which is no longer needed and which Energy Action is not required by law to retain. Documents will be kept for the period of time as required by law.

Our website contains links to the websites of third parties over which we have no influence in regards to their compliance with Principles or content. Please be aware that Energy Action is not responsible for the compliance by these third parties with their obligations concerning your personal information. You should review the Privacy Policy of any website that you access through the Energy Action website.

10.0 Authorities and Responsibilities

The Risk Management & Audit Committee (**RMAC**) will be responsible to ensure that appropriate policies are in place to protect the privacy of all personal information about clients, customers or other individuals that is collected or held by Energy Action.

Executive Officers and Managers will be responsible for ensuring that appropriate privacy procedures are implemented and adhered to, to achieve the highest possible levels of privacy and security for customers, shareholders and client information.

11.0 Complaints

Energy Action has an established internal dispute resolution system in place to efficiently manage enquiries and complaints. If you wish to make an enquiry or lodge a complaint in relation to how Energy Action handles your personal information you should in the first instance contact Energy Action using the following details:

Post: Energy Action Limited - Marketing

Level 5, 56 Station Street Parramatta NSW 2150

Telephone: 1300 553 551 or (02) 9633 6400

Fax: (02) 9475 0954

Email: marketing@energyaction.com.au

A representative of Energy Action will respond to let you know who will be handling your matter and when you can expect a further response.

If you feel that we have not adequately dealt with your complaint or that it cannot be solved internally, you may refer the matter to the Office of the Australian Information Commissioner who can be contacted online at www.oaPurpose of the Bill

The purpose of the Privacy Amendment (Notifiable Data Breaches) Bill 2016 (the Bill) is to amend the *Privacy Act 1988* in order to introduce mandatory data breach notification provisions which will apply to entities currently subject to the *Privacy Act*, namely most Commonwealth Government agencies, some private sector organisations ('entities'), credit reporting bodies, credit providers and tax file number recipients.

Structure of the Bill

The Bill contains one Schedule of amendments to the *Privacy Act*. The main amendment in Schedule 1 is **item 3** which inserts a **new Part IIIC**, titled 'Notification of eligible data breaches'. This new Part contains the substantive elements of the mandatory data breach notification provisions, which apply to entities that are regulated by the *Privacy Act*.

The **new Part IIIC** is divided into three Divisions. Broadly, the first Division sets out preliminary general matters including relevant definitions and application provisions, the second Division sets out when an 'eligible data breach' will have occurred and the third Division contains obligations for entities to notify that such a data breach has occurred, subject to certain exceptions.

Background

Data breach notifications

As the Explanatory Memorandum notes, mandatory data breach notification commonly refers to:

... a legal requirement to provide notice to affected individuals and the relevant regulator when certain kinds of security incidents compromise information of a certain kind or kinds. In some jurisdictions, notification is also only required if the data breach meets a specified harm threshold. Examples of when data breach notification may be required could include a malicious breach of the secure storage and handling of information (e.g. in a cyber security incident), an accidental loss (most commonly of IT equipment or hard copy documents), a negligent or improper disclosure of information, or otherwise, where the incident satisfies the applicable harm threshold (if any).[1]

Data breach notification has been a topical issue in privacy regulation around the world for some years, with concerns about identity theft and identity fraud driving the development of new laws in this area.[2]

The Privacy Act *and data breaches*

The Australian Privacy Principles (APPs), which are contained in Schedule 1 of the *Privacy Act*, outline how most Australian Government agencies, all private sector and not-for-profit organisations with an annual turnover of more than $3 million, all private health service providers and some small businesses (collectively called 'APP entities') must handle, use and manage personal information.

Currently, the *Privacy Act* does not impose an obligation on entities to notify the Australian Information Commissioner (the Commissioner) or any individuals whose personal information has been compromised. However, APP 11 requires that agencies and organisations take reasonable steps to maintain the security of the personal information they hold from misuse, interference and loss, and from unauthorised access, modification or disclosure. Other provisions in the *Privacy Act* create equivalent obligations in relation to credit reporting information, credit eligibility information and tax file number information.[3]

The Office of the Australian Information Commissioner (OAIC) currently has in place a voluntary guide for entities giving advice on how to handle a data breach.[4] Although not mandatory, entities regulated by the *Privacy Act* are encouraged to comply with this guide so as to 'voluntarily put in place reasonable measures to deal with data breaches (including notification of affected individuals and the OAIC), while legislative change is considered by the Australian Government'.[5] The Commissioner has stated that he continues to support the introduction of a mandatory data breach

reporting scheme for serious data breaches noting that the OAIC continues to see evidence of a high number of serious data breaches. He quotes the *McAfee Labs Threat Report* for August 2015, which reviewed changes in cyber threats and cybersecurity from 2010 to 2015 and which states that there has been a 'monumental increase in the number of major data breaches and in the volume of records stolen'.[6] In the Commissioner's view a mandatory notification scheme is necessary to:

- give confidence to all Australians that if they are affected by serious data breach, they will be given a chance to protect their interests, and
- signal to entities that protection of individuals' personal information should be a priority in the digital age.[7]

Australian Law Reform Commission: report

The Australian Law Reform Commission (ALRC) in its 2008 report on privacy, *For Your Information: Australian Privacy Law and Practice* (the ALRC Report), considered the topic of data breach notification and made a recommendation regarding the establishment of a mandatory notification scheme. The ALRC noted that, with advances in technology, entities were increasingly holding larger amounts of identifying information in electronic form, raising the risk that a breach of this information could result in another individual using the information for identity theft and identity fraud. A notification requirement for entities that suffer data breaches would allow individuals whose personal information had been compromised by the breach to take remedial steps to lessen the adverse impact that might arise from the breach.[8] The ALRC recommended that the *Privacy Act* be amended to impose a mandatory obligation to notify the Privacy Commissioner and affected individuals in the event of a data breach that could give rise to a real risk of serious harm to affected individuals. Notification would be compulsory unless it would impact upon a law enforcement investigation or was determined by the regulator to be contrary to the public interest. Failure to notify would attract a civil penalty.[9]

Parliamentary Joint Committee on Intelligence and Security: reports

Recommendations regarding a mandatory data breach notification scheme were also made as part of the Parliamentary Joint Committee on Intelligence and Security (PJCIS) inquiries into a mandatory data retention regime. Firstly in May 2013, the PJCIS released a *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*. The report recommended that, if a mandatory data retention regime should proceed, its introduction should include the introduction of a robust mandatory data breach notification scheme.[10]

Again, in February 2015 the PJCIS in its *Advisory report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014* (the Data Retention Bill 2014) recommended the introduction of a mandatory data breach notification scheme by the end of 2015.[11]

The three Bills

Since 2008 when mandatory data breach notification was first recommended by the ALRC, there have been three different Bills that would establish a mandatory data breach notification scheme:

- Privacy Amendment (Privacy Alerts) Bill 2013[12]
- exposure draft of the Privacy Amendment (Notification of Serious Data Breaches) Bill 2015[13]
- the current Bill.

Privacy Amendment (Privacy Alerts) Bill 2013

On 29 May 2013 the then Labor Government introduced the Privacy Amendment (Privacy Alerts) Bill 2013 (2013 Bill) into Parliament. The Bill was intended to implement ALRC recommendation 51–1 and to strengthen the existing voluntary data breach notification framework in order to counter underreporting of data breaches and to help prevent or reduce the effects of serious crimes like identity theft. The Bill passed the House of Representatives with bipartisan support. It was referred to Committee but lapsed on prorogation of the 43rd Parliament.[14]

Exposure draft: Privacy Amendment (Notification of Serious Data Breaches) Bill 2015

On 3 March 2015 the Coalition Government, as part of its response to the PJCIS report on the Data Retention Bill 2014, agreed to introduce a mandatory data breach notification scheme by the end of 2015 and to consult on draft legislation.[15] In December of that year, the Attorney-General released an exposure draft of the Privacy Amendment (Notification of Serious Data Breaches) Bill 2015 (the 2015 exposure draft) and a discussion paper for public submission. Forty-seven public submissions were received before submissions closed on 4 March 2016.[16]

The 2015 exposure draft was similar to the 2013 Bill in that it applied the same threshold test for when an entity would be required to notify a 'serious data breach' and imposed similar data breach notification requirements. There were a range of views in submissions—a common theme being that the legislation needed further explanation and clarification on how to determine when a serious data breach might occur.

The current Bill

The current Bill, introduced on 19 October 2016, is based on the 2015 exposure draft but includes significant amendments. In particular it introduces a higher threshold test for when data breach notification is mandatory, and provides other changes aimed at reducing and streamlining the need for notification. Many of these changes would appear to be responding to recommendations from the various submissions on the 2015 exposure draft.

Further discussion on the differences between the three Bills is found in the *Key issues and provisions* section below.

Committee consideration

At the time of writing the Bill had not been referred to a parliamentary committee for inquiry and report.

Senate Standing Committee for the Scrutiny of Bills

The Committee has considered the Bill and noted that it includes a number of exceptions to the mandatory data breach notification provisions:

These exceptions limit the right to privacy as in such circumstances individuals will not be notified of an eligible data breach if one of the exceptions apply.[17]

However, the Committee chose not to make any further comment in relation to this matter given the detailed discussion about any limitation on the right to privacy contained in the explanatory material.[18]

Policy position of non-government parties/independents

From the time of its response to the 2008 ALRC Report on privacy, the Labor Party has consistently supported mandatory data breach notification. While in Government, Labor initiated the first legislation in 2013.

The Shadow Attorney-General Mark Dreyfus has been critical of the current Government's delay in introducing legislation stating:

It has only taken Attorney-General George Brandis three years, but he has finally caught up with Labor's proposed legislation for mandatory notification of consumers when their personal data has been breached.[19]

At the time of writing this Bills Digest, the Labor Party had not provided any public comment on the current Bill, however, in August prior to the tabling of the Bill, the shadow Attorney-General called on the Government to negotiate with Labor on the proposed legislation to ensure a speedy passage through Parliament.

Mr Dreyfus also cautioned the Government against bending to the wishes of the banking industry on this matter stating:

ic.gov.au, by phoning 1300 363 992 or emailing enquiries@oaic.gov.au.