Our reference: FOIREQ24/00352

CR

By email: foi+request-11183-7373c2f0@righttoknow.org.au

Freedom of Information Request – FOIREQ24/00352

Dear CR

I refer to your request for access to documents made under the *Freedom of Information Act 1982* (CT) (the FOI Act). Your Freedom of Information request (FOI request) was received by the Office of the Australian Commissioner (OAIC) on 5 July 2024.

I am writing to inform you of my decision.

I have identified one document within the scope of your request. I have made a decision to:

- grant access in part to one document.

In accordance with section 26(1)(a) of the FOI Act, the reasons for my decision and findings on material questions of fact are provided below.

Background

Scope of your request

Your FOI request sought access to the following information:

Following our recent correspondence, I have decided to submit a new FOI request. I request access to the following documents under the Freedom of Information Act 1982:

1. *Data breach reports from 1 January 2020 to 5 July 2024 where the respondent's sector is government (local, state, and federal government).*
   - *The required document is similar to the one released in FOIREQ24/00132.*
   - *Respondent names are to be included in the scope of this request.*

I respectfully submit that disclosing agency names is strongly aligned with the public interest, as evidenced by the OAIC's Australian Community Attitudes to Privacy Survey 2023:

- *Only two in five Australians feel most organisations they deal with are transparent about how they handle their information. Disclosing the agency names would serve the public interest by providing transparency and accountability around how government agencies are managing data breaches.*
- *82% of Australians actively care about protecting their personal information. Knowing which agencies have experienced breaches empowers them to make informed decisions about their interactions with those agencies.*
- *Three-quarters of Australians feel data breaches are one of the biggest privacy risks they face today. Identifying the agencies involved allows for more nuanced public debate and scrutiny of this critical issue.*
- *After quality and price, data privacy is the third most important factor when choosing a product or service. Disclosing the agency names would further empower Australians to make well-informed decisions when accessing government services.*

For these reasons, I believe the public interest factors strongly favour the disclosure of the respondent names in the requested data breach reports. I hope you will give this new FOI request your careful consideration. Please let me know if you require any further information from me.

Following consultation with you on the scope of your request, on 11 July 2024 you revised your request to be as follows:

> *I am seeking data breach reports made under the Notifiable Data Breaches scheme. The same document as released in FOIREQ24/00132.*

Request timeframe

Your request was made on 5 July 2024.

This means that a decision on your request is due by 5 August 2024.

Decision

I am an officer authorised under section 23(1) of the FOI Act to make decisions in relation to FOI requests on behalf of the OAIC.

Subject to the following provisions of the FOI Act, I have made a decision to:

- grant access in part to one document.

Searches Undertaken

The FOI Act requires that all reasonable steps have been taken to locate documents within scope of an FOI request.

The following line areas of the OAIC conducted reasonable searches for documents relevant to you request:

- Notifiable Data Breaches Team

Searches were conducted across the OAIC's various document storage systems including:

- the OAIC's case management system - Resolve

The following search terms were used when undertaking electronic records searches:

- Notifiable Data Breach Reports within defined time period of 1 January 2020 to 5 July 2024.

Having consulted with the relevant line areas and undertaken a review of the records of the various search and retrieval efforts, I am satisfied that a reasonable search has been undertaken in response to your request.

Reasons for decision

Material taken into account

In making my decision, I have had regard to the following:

- your FOI request dated 5 July 2024 and subsequent revised scope dated 11 July 2024
- the FOI Act, in 3, 11, 11A, 15, 17, 22, 26 and 47E(d) of the FOI Act
- the Guidelines issued by the Australian Information Commissioner under section 93A of the FOI Act to which regard must be had in performing a function or exercising a power under the FOI Act (FOI Guidelines)

Access to edited copies with irrelevant and exempt matter deleted (section 22)

In accordance with section 22 of the FOI Act, an agency must consider whether it would be reasonably practicable to prepare an edited copy of documents subject to

an FOI request where material has been identified as exempt or irrelevant to the request.

I have determined that FOI Act exemptions apply to this material. Accordingly, the exempt material has been removed in accordance with s 22(1)(a)(i) of the FOI Act.

I have also identified the following material within the documents to be irrelevant or out of scope of your request in accordance with s 22(1)(a)(ii) of the FOI Act:

- material related to non-Government entities which have been included as part of the bundle because of a system error when creating the Resolve report.

Accordingly, I have made an edited copy of the document which removes this material in accordance with s 22 of the FOI Act and otherwise grants you **access in part** to the material in scope of your request.

Creation of a document in response to your FOI request (section 17)

Pursuant to section 17 of the FOI Act, I have made a decision to create one document in response to your request. I have made a decision to grant access in part to this one document.

Under section 17 of the FOI Act, if an FOI request is made for a document that could be produced by using a computer ordinarily available to the agency for retrieving or collating stored information, an agency is required to deal with the request as if it was a request for written documents to which the FOI Act applies.

The FOI Guidelines [at 3.204] explain that section 17 may require an agency to produce a written document of information that is stored electronically and not in a discrete written form, if it does not appear from the request that the applicant wishes to be provided with a computer tape or disk on which the information is recorded. The obligation to produce a written document arises if:

- the agency could produce a written document containing the information by using a computer or other equipment that is ordinarily available' to the agency for retrieving or collating stored information (section 17(1)(c)(i)), or making a transcript from a sound recording (section 17(1)(c)(ii)); and
- producing a written document would not substantially and unreasonably divert the resources of the agency from its other operations (section 17(2)).

If those conditions are met, the FOI Act applies as if the applicant had requested access to the written document and it was already in the agency's possession.

Your request sought access to data breach reports made under the Notifiable Data Breaches scheme. The Notifiable Data Breach Team advised me that the material sought is not available in a discrete form but instead is able to be produced in a written document through the use of a computer.

In light of this, a document has been created under section 17 in response to your request and is included in the schedule of documents attached.

Section 47E(d) – Proper and efficient conduct of the OAIC's operations

In accordance with section 47E(d) of the FOI Act, I have made a decision to redact material on the basis that disclosure would or could reasonably be expected to have a substantial adverse effect on the proper and efficient conduct of the OAIC's operations.

Paragraph 6.101 of the FOI Guidelines explains that:

> *For the grounds in ss 47E(a)–(d) to apply, the predicted effect needs to be reasonably expected to occur. The term 'could reasonably be expected' is explained in greater detail in Part 5. There must be more than merely an assumption or allegation that damage may occur if the document were to be released.*

Additionally, at 6.103 the FOI Guidelines further explain:

> *An agency cannot merely assert that an effect would occur following disclosure. The particulars of the predicted effect should be identified during the decision making process, including whether the effect could reasonably be expected to occur. Where the conditional exemption is relied upon, the relevant particulars and reasons should form part of the decision maker's statement of reasons, if they can be included without disclosing exempt material (s 26, see Part 3).*

The term 'substantial adverse effect' is explained in the Guidelines (at [5.20]) and it broadly means 'an adverse effect which is sufficiently serious or significant to cause concern to a properly concerned reasonable person'. The word 'substantial', taken in the context of substantial loss or damage, has been interpreted as 'loss or damage that is, in the circumstances, real or of substance and not insubstantial or nominal'.

The material that I have decided is subject to conditional exemption comprises of information given by Government agencies to the OAIC in the course of notifying the OAIC of suspected or actual data breaches, as well as the OAIC's unique identification numbers for each matter, and some classification information which would render agencies reasonably identifiable.

In undertaking an assessment of this conditional exemption, I have had regard to relevant and recent AAT and Information Commissioner decisions including *Seven Network Operations Limited and Australian Human Rights Commission* [2021] AICmr 66, *Paul Farrell and Department of Home Affairs (Freedom of information)* (No 2) [2022] AICmr 49 (8 April 2022).

In *Paul Farrell and Department of Home Affairs (Freedom of information)* (No 2) [2022] AICmr 49 (8 April 2022), whilst the material found within the documents related to the Department of Home Affairs' operations, the Commissioner determined that the Department had failed to provide sufficient evidence as to why disclosure would have a substantial and adverse effect on its operations. This decision further reinforces the position that this provision requires a high threshold as to the substantial and adverse effect that disclosure would have on an agency's operations.

In order to determine whether disclosure would, or could reasonably be expected to, have a substantial adverse effect on the proper and efficient conduct of the operations of the OAIC, I have taken into consideration the functions and activities of the OAIC.

The OAIC is an independent statutory agency within the Attorney-General's portfolio, established under the *Australian Information Commissioner Act 2010* (Cth). The OAIC comprises the Australian Information Commissioner (office currently held by Angelene Faulk), the Privacy Commissioner (office currently held by Carly Kind), the FOI Commissioner (office currently held by Elizabeth Tydd), and the staff of the OAIC.

The OAIC performs a range of functions pursuant to both the *Privacy Act 1988 (Cth)* ('*Privacy Act*'), and the *Freedom of Information Act 1982.* Of particular note in this matter, the OAIC exercises a range of functions and powers that relate to the Notifiable Data Breaches (NDB) Scheme as set out in the *Privacy Act*. These functions and powers include:

- receiving notifications of eligible data breaches;
- encouraging compliance with the NDB Scheme, including by handling complaints, conducting investigations and taking other regulatory action;
- offering advice and guidance to regulated entities; and
- providing information to the community about the operation of the NDB Scheme.

The *Privacy Act* is a voluntary scheme; however, entities are required to, at a minimum, provide the following information:

- the identity and contact details of the entity;
- a description of the eligible data breach;
- the particular kind or kinds of information concerned; and

- recommendations about the steps that individuals should take in response to the eligible data breach.

The OAIC's website recommends reporting entities also provide the following information to assist the OAIC to understand the breach: [1]

- the dates the breach occurred and when it was discovered;
- the cause of the breach;
- how the breach occurred;
- the number of individuals whose personal information was involved;
- whether any remedial action has been taken;
- how individuals will be notified; and
- whether the data breach has been reported to any other data protection authorities, law enforcement bodies or regulatory bodies.

The OAIC website also advises reporting entities that "…[t]he more information you tell us about the circumstances of the data breach, what you've done to contain the data breach and any remedial action you've taken, will help us respond to your notification" and that "[t]he OAIC may need to contact you to seek further information" if this information is not provided. The OAIC then relies on the information provided by the entities to consider whether further regulatory action, if any, is required.

As such, I consider that the disclosure of material provided to the OAIC in instances of data breaches could reasonably be expected to undermine the agency's ability to receive timely, frank and full disclosure of information from entities including government agencies that have experienced or have reasonable grounds to believe that they have experienced, an eligible data breach. In addition, I consider that the release of this material could reasonably be expected to delay the OAIC's ability to take further regulatory action in response to an eligible data breach (if required) as entities could be reluctant to provide timely, frank and full disclosure of information to the OAIC if the information they provide, and their respective identities may be publicly disclosed.

For these reasons, I consider that disclosure of material comprising of information given by Government agencies to the OAIC in the course of notifying the OAIC of suspected or actual data breaches, as well as the OAIC's unique identification numbers for each matter, and some classification information which would render agencies reasonably identifiable would, or could reasonably be expected to substantially and adversely affect the proper and efficient conduct of the OAIC's

[1] Report a Data Breach | OAIC

functions under the NDB Scheme in the future. As such, I consider this material is conditionally exempt under s 47E(d) of the FOI Act.

As section 47E of the FOI Act is a conditional exemption, I am also required to consider the application of a public interest test.

My consideration of the public interest test, in respect of the material subject to conditional exemption in the documents is discussed below.

Application of the public interest test – (section 11A and 11B)

As provided above, I have considered that material within the document is subject to conditional exemption under s 47E(d).

Section 11A(5) provides that where a document is considered to be conditionally exempt, an agency **must** give the person access to that document unless the FOI decision maker would, on balance, would be contrary to the public interest.

This means that I must balance factors for and against disclosure in light of the public interest.

In Chapter 6, the FOI Guidelines provide the following guidance:

*6.4 There is a **single public interest test to apply to each of the conditional exemptions.** This public interest test is defined to include certain factors that must be taken into account where relevant, and some factors which must not be taken into account.*

6.5 The public interest test is considered to be:

- *something that is of serious concern or benefit to the public, **not merely of individual interest***
- ***not something of interest to the public, but in the public interest***
- *not a static concept, where it lies in a particular matter will often depend on a balancing of interests*
- *necessarily broad and non-specific, and*
- *related to matters of common concern or relevance to all members of the public, or a substantial section of the public.*

6.6 It is not necessary for a matter to be in the interest of the public as a whole. It may be sufficient that the matter is in the interest of a section of the public bounded by geography or another characteristic that depends on the particular situation. A matter of public interest or benefit to an individual or

small group of people may also be a matter of general public interest.

In the AAT case of *Utopia Financial Services Pty Ltd and Australian Securities and Investments Commission (Freedom of information)* [2017] AATA 269, at paragraph 133 of the Decision Deputy President Forgie explained that:

> … the time at which I make my decision for section 11A(5) requires access to be given to a conditionally exempt document "*at a particular time*" unless doing so is, on balance, contrary to the public interest. Where the balance lies may vary from time to time for it is affected not only by factors peculiar to the particular information in the documents but by factors external to them.

The FOI Act sets out four factors favouring access, which must be considered if relevant. Of these factors, we consider the following to be relevant:

- promote the objects of the FOI Act, and
- inform debate on a matter of public importance.

In addition to these factors favouring disclosure, I have also considered that the following factors in favour of disclosure apply:

- disclosure would enhance scrutiny around government decision making, and
- disclosure would better inform a matter of public importance or debate.

Section 11B(4) of the FOI Act provides factors which are not to be taken into account in , which I have had regard to. Section 11B does not further prescribe the factors against disclosure to be considered. In considering the documents subject to this request, I consider that the follow factors do not favour disclosure:

- disclosure would have an adverse effect on the OAIC's proper and efficient operations relating to receiving full and frank disclosure of actual or suspected data breaches from Australian Government agencies;
- disclosure would undermine the confidence and trust in the OAIC as a regulator to deal with matters it regulates in a sensitive and timely manner;
- disclosure would reasonably be expected to delay the OAIC's consideration of, and ability to, take further regulatory action in response to an eligible data breach if entities are reluctant to provide timely, full and frank information if their respective identities may be disclosed; and
- in case of a breach which meets the requisite threshold of 'serious harm', entities regulated by the *Privacy Act* are required to notify individuals affected by an eligible data breach of the nature of the breach, inclusive of the type of information captured in their reporting to the OAIC.

I note you provided several reasons as to why you consider the release of agency names remains in the public interest. The reasons you provided are as follows:

- *Only two in five Australians feel most organisations they deal with are transparent about how they handle their information. Disclosing the agency names would serve the public interest by providing transparency and accountability around how government agencies are managing data breaches.*
- *82% of Australians actively care about protecting their personal information. Knowing which agencies have experienced breaches empowers them to make informed decisions about their interactions with those agencies.*
- *Three-quarters of Australians feel data breaches are one of the biggest privacy risks they face today. Identifying the agencies involved allows for more nuanced public debate and scrutiny of this critical issue.*
- *After quality and price, data privacy is the third most important factor when choosing a product or service. Disclosing the agency names would further empower Australians to make well-informed decisions when accessing government services.*

Whilst I agree that the release of agency names who have reported an actual or suspected notifiable data breach to the OAIC would increase transparency and accountability is of the public interest, I consider the requisite transparency and accountability requirements to be sufficiently met when the agency complies with their notification requirements under the *Privacy Act*.

As set out above, agencies who are subject to a data breach which is likely to result in 'serious harm' to the individuals of whose information is affected are required to notify these individuals of the breach. Sections 26WK(3) of the *Privacy Act* requires an entity to notify the individuals who are or are at risk of being affected by the breach of:

- the nature of the data breach,
- the type of information implicated in the data breach, and
- recommendations of steps that should be taken in response to the data breach, to further protect their data.

A copy of this statement must be provided to the individuals of whom are affected as soon as reasonably practicable after the breach is identified.[2]

[2] Section 26WK(2) of the *Privacy Act*.

Where it is not reasonably practicable to provide this statement to each affected individual, for example, if the class of data breached is so broad that it is impractical to contact each affected individual directly, the agency must take reasonable steps to publish this information on their website, and to the world at large.[3] This often includes reporting on the details of the breach, inclusive of the name of agency, via mainstream media outlets.

The agencies' first and foremost obligations are to the individuals who are affected by the data breaches, to take adequate measures to detect, respond and advise these individuals. As outlined in my decisions above, in my view based on the information before me at this time, I have concerns that disclosure of the nature and specific details of the information in a public forum such as via Right to Know, is likely to prejudice the abilities of these agencies in responding to the data breaches, and the OAIC's ability to gather similar information to assess these breaches in the future.

I acknowledge that Australians consider data breaches are one of the most serious privacy risks faced today, and that there is a significant public interest in informing the public about data breaches and their impact. I also acknowledge that such public interest compels discussion, debate and scrutiny around how entities and agencies manage data breaches.

However, I consider that it is of greater public interest that the OAIC is able to fully engage with agencies who are subject to eligible data breaches in order to effectively execute its role as a regulator. I consider the OAIC's ability to receive timely, full and frank information about the nature, cause and impacts of a breach paramount to its role as the privacy regulator in Australia. Agencies are likely to be reticent to provide the OAIC with all of this information where there is a likelihood such information could be published to the world at large. Without receipt of this information in a timely manner, the OAIC's role in assisting with rectification measures will be hindered.

Having balanced the abovementioned factors against the public interest in protecting the proper and efficient conduct of the OAIC's function under the NDB Scheme, I consider that disclosure could reasonably be expected to have an adverse effect on the OAIC's ability to receive timely, full and frank disclosures from agencies who experience, or suspect to have experienced, an eligible data breach where there is a likelihood that their respective identities may be publicly disclosed. I consider the release of information provided to the OAIC in the course of the required disclosures would undermine confidence in the agency, likely resulting in delayed

[3] Section 26WL(2)(c) of the *Privacy Act.*

information being provided. This would further impact upon the OAIC's ability to assess the reports made and could be reasonably expected to delay the consideration of, and ability to, take further regulatory action in response, if required.

On balance, I consider the public interest factors against disclosure to be more persuasive than the public interest factors favouring disclosure. I am therefore satisfied that it is in the public interest to withhold the exempt material.

Disclosure log decision

Section 11C of the FOI Act requires agencies to publish online document released to members of the public within 10 days of release, except if they contain personal or business information that would be unreasonable to publish.

I have made a decision to publish the documents subject to your request on the OAIC's disclosure log.

Release of document

The documents are enclosed for release.

Please see the following page for information about your review rights.

Yours sincerely,

Tahlia
Lawyer

5 August 2024

If you disagree with my decision

Internal review

You have the right to apply for an internal review of my decision under Part VI of the FOI Act. An internal review will be conducted, to the extent possible, by an officer of the OAIC who was not involved in or consulted in the making of my decision. If you wish to apply for an internal review, you must do so in writing within 30 days. There is no application fee for internal review.

If you wish to apply for an internal review, please mark your application for the attention of the FOI Coordinator and state the grounds on which you consider that my decision should be reviewed.

Applications for internal reviews can be submitted to:

> Office of the Australian Information Commissioner
> GPO Box 5218
> SYDNEY NSW 2001

Alternatively, you can submit your application by email to foi@oaic.gov.au, or by fax on 02 9284 9666.

Further review

You have the right to seek review of this decision by the Information Commissioner and the Administrative Appeals Tribunal (AAT).

You may apply to the Information Commissioner for a review of my decision (IC review). If you wish to apply for IC review, you must do so in writing within 60 days. Your application must provide an address (which can be an email address or fax number) that we can send notices to, and include a copy of this letter. A request for IC review can be made in relation to my decision, or an internal review decision.

It is the Information Commissioner's view that it will usually not be in the interests of the administration of the FOI Act to conduct an IC review of a decision, or an internal review decision, made by the agency that the Information Commissioner heads: the OAIC. For this reason, if you make an application for IC review of my decision, and the Information Commissioner is satisfied that in the interests of administration of the Act it is desirable that my decision be considered by the AAT, the Information Commissioner may decide not to undertake an IC review.

Section 57A of the FOI Act provides that, before you can apply to the AAT for review of an FOI decision, you must first have applied for IC review.

Applications for IC review can be submitted online at: https://forms.business.gov.au/smartforms/servlet/SmartForm.html?formCode=ICR_10

Alternatively, you can submit your application to:

> Office of the Australian Information Commissioner
> GPO Box 5218
> SYDNEY NSW 2001

Or by email to foidr@oaic.gov.au, or by fax on 02 9284 9666.

Accessing your information

If you would like access to the information that we hold about you, please contact foi@oaic.gov.au. More information is available on the Access our information page on our website.