Australian Government
Office of the Australian Information Commissioner

Our reference: FOIREQ24/00423

CR

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

Internal review decision – FOIREQ24/00423

Dear CR

I refer to your request for internal review of a decision of the OAIC relating to a request for access to documents made under the *Freedom of Information Act 1982* (Cth) (the FOI Act).

The original decision was made by Tahlia Pelaccia, Lawyer, on 5 August 2024. The decision created and granted access in part to one document.

An internal review is a fresh decision made by a person other than the person who made the original decision (section 54C of the FOI Act). All materials available to the original decision maker have been made available to me.

I have made a decision to vary the decision and grant further access in part to the one document.

Background

Your original FOI request

Your FOI request dated 5 July 2024 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 as follows:

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

On 5 August 2024 the original decision maker made a decision to create and grant access in part to one document.

This decision was made subject to the conditional exemption contained in section 47E(d) of the FOI Act (proper and efficient conduct of the OAIC's operations).

Your internal review request

On 26 August 2024 you wrote to the OAIC requesting an internal review of this decision.

Your internal review request was on the following terms:

> *1. I disagree with the decision-maker's 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. Please refer to the decision-maker's statements.*
>
> *i. It is possible that disclosing this information would encourage the OAIC to act more quickly, as it would be subject to public scrutiny.*
>
> *ii. The decision-maker's concern that government agencies might be reticent to provide information if their identities are revealed is unfounded, as the legal obligation to report eligible data breaches would remain unchanged.*

iii. The decision-maker implies that disclosure could discourage government agencies from providing voluntary information beyond the minimum requirements. The reliance on voluntary information is misplaced. The FOI Act aims to ensure access to information, not incentivise voluntary disclosure. The public's right to know should not be contingent on the goodwill of government agencies. Furthermore, the OAIC can address any concerns about voluntary disclosure through other means, such as providing guidance or incentives for comprehensive reporting.

iv. If there was an actual impact on the proper and efficient conduct of the OAIC's operations, it would not rise to the level of 'substantial and adverse'.

2. The decision-makers application of the public interest test was flawed for the following reasons:

2.1 The decision-maker failed to consider the following factors in favour of disclosure:

i. Disclosure would allow the public to make better-informed decisions about their interactions with government agencies. Currently, there is no way an individual can consider an individual government agency's track record of data privacy and security when deciding whether to share their personal information or not. I note that the OAIC publishes aggregate data in its Notifiable Data Breaches Report. However, the public interest in understanding the specific risks associated with individual agencies is not adequately served by aggregate data alone.

ii. Disclosure would allow or assist inquiry into possible deficiencies in the conduct or administration of an agency. [FOI Guidelines 6.231] iii. Disclosure could reveal deficiencies in privacy legislation. [FOI Guidelines 6.231]

2.2 The decision-maker incorrectly considered the following factors that do not favour disclosure:

A) The decision maker states, "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."

i. The frankness and candour argument in the FOI context has been discussed in numerous previous decisions of the Information Commissioner, the AAT, and the courts. Public servants 'are expected to operate within a framework that encourages open access to information and recognises Government information as a national resource to be managed for public purposes'. The FOI Guidelines refer to the FOI Act recognising that Australia's democracy is strengthened when the public is empowered to participate in Government processes and scrutinise Government activities. The FOI Guidelines further state that 'In this setting, transparency of the work of public servants should be the accepted operating environment and fears about a lessening of frank and candid advice correspondingly diminished.'

B) The decision maker states, "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."

i. 'Access to the document could result in embarrassment to the Commonwealth Government, or cause a loss of confidence in the Commonwealth Government' is an irrelevant factor as described in s 11B(4) of the FOI Act and therefore was incorrectly considered in the public interest test.

C) The decision maker states, "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."

i) As previously stated, government agencies should start with the assumption that public servants are obliged by their position to always provide robust and frank advice and that obligation will not be diminished by the transparency of government activities.

D) The decision maker states, "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. This is not relevant to the public interest test.

ii. I note that the decision-maker explains that individuals directly affected by data breaches are notified of the breach, however, the public interest extends beyond individual impact. Data breaches have systemic consequences, such as undermining public trust in government agencies or exposing vulnerabilities in critical infrastructure. By disclosing agency names, the public can engage in informed discussions about these broader implications and advocate for policy changes to improve data security.

2.3 The public interest in transparency and accountability outweighs any potential harm to the OAIC's operations. Given the high level of public concern about data breaches and the importance of government transparency, the public interest in knowing which agencies are responsible for these breaches is significant. This interest outweighs any speculative harm to the OAIC's operations. This information is crucial for informed public debate, holding agencies accountable, and assessing the effectiveness of government data protection measures. The OAIC's role is to protect the privacy of Australians, and this includes providing them with the information they need to make informed decisions about their interactions with government agencies.

3. The decision-maker states, "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) The forum of an FOI request is irrelevant to the decision to deny access to information. FOI applicants have the right to publish disclosed information, and the disclosed documents become accessible to the public via the OAIC's to disclosure log.

A decision on your internal review request is due on 25 September 2024.

Consultation

The original decision maker did not undertake consultation with other government agencies or third parties in relation to documents falling within scope of your request. I have undertaken consultation with approximately 90 government agencies named in the document and taken their responses into account in this decision.

Decision

I am an officer authorised under s 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 vary the decision and grant further access in part to one document.

I have upheld the original decision to exempt the material in columns 5-7 of the document under s 47E(d), but have decided that only some of the agency names and OAIC reference numbers (contained in columns 1 and 3) are exempt under s 47E(d).

I have also found some additional material to be irrelevant or out of scope under s 22(1)(a)(ii) of the FOI Act.

Reasons for decision

Materials 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;
- your internal review request dated 26 August 2024;
- the FOI Act, in particular sections 3, 11, 11A, 15, 17, 22, 26 and 47E(d) of the FOI Act;
- the Guidelines issued by the Australian Information Commissioner under s 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); and

- consultation with line areas of the OAIC and other government agencies in relation to 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 3.210] 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 (**NDB**) Scheme. The OAIC's NDB 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.

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 was included as part of the report because of a system error when creating the Resolve report;
- further material related to non-Government entities which was included as part of the report because of incorrect categories being applied in the OAIC's Resolve system.

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.

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 grant access in part to the document created under section 17 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 6.14-6.16 of the FOI Guidelines explains the test of "would or could reasonably be expected to" as follows:

> *6.14 The test requires the decision maker to assess the likelihood of the predicted or forecast event, effect or damage occurring after disclosure of a document.*
>
> *6.15 The use of the word 'could' is less stringent than 'would' and requires analysis of the reasonable expectation rather than the certainty of an event, effect or damage occurring. It may be a reasonable expectation that an effect has occurred, is presently occurring, or could occur in the future.*
>
> *6.16 The mere risk, allegation, possibility, or chance of prejudice does not qualify as a reasonable expectation. There must be, based on reasonable grounds, at least a real, significant or material possibility of prejudice.*

The material I have determined is conditionally exempt under section 47E(d) of the FOI Act is:

- for **all breaches**, the details of the breach and the kinds of personal information affected by the breach; and
- for **some breaches**, the specific agency reference number assigned to the breach, the agency name.

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 (***Seven Network***), *Paul Farrell and Department of Home Affairs (Freedom of information)* (No 2) [2022] AICmr 49 and *Knight v Commonwealth Ombudsman* [2021] AATA 2504.

In *Seven Network*, a document was found not to be conditionally exempt under section 47E(d) of the FOI Act in circumstances where the agency argued that disclosure of the relevant material would or could reasonably be expected to have result in stakeholders declining to work with the Australian Human Rights Commission. The decision found that there was not sufficient evidence to support the conclusion that such harm would occur. This decision 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.

I note that in your request for internal review dated 26 August 2024 you both disagree that the disclosure of this information could have an impact on the operations of the OAIC and that even if it did have an impact, it would not rise to the level of substantial and adverse as follows:

> *1. I disagree with the decision-maker's 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. Please refer to the decision-maker's statements.*
>
> *i. It is possible that disclosing this information would encourage the OAIC to act more quickly, as it would be subject to public scrutiny.*
>
> *ii. The decision-maker's concern that government agencies might be reticent to provide information if their identities are revealed is unfounded, as the legal obligation to report eligible data breaches would remain unchanged.*
>
> *iii. The decision-maker implies that disclosure could discourage government agencies from providing voluntary information beyond the minimum requirements. The reliance on voluntary information is misplaced. The FOI Act aims to ensure access to information, not incentivise voluntary disclosure. The public's right to know should not be contingent on the goodwill of government agencies. Furthermore, the OAIC can*

address any concerns about voluntary disclosure through other means, such as providing guidance or incentives for comprehensive reporting.

iv. If there was an actual impact on the proper and efficient conduct of the OAIC's operations, it would not rise to the level of 'substantial and adverse'.

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. I have also had regard to your submissions and consultation with the OAIC's NDB team and affected agencies.

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 Elizabeth Tydd), the Privacy Commissioner (office currently held by Carly Kind), and the FOI Commissioner (office currently held by Toni Pirani), and the staff of the OAIC. Relevant to this matter, the OAIC is responsible for administering the NDB Scheme under Part IIIC of the *Privacy Act 1988* (Cth) (**Privacy Act**).

The OAIC'S functions and powers in administering the NDB Scheme include:

- receiving notifications of eligible data breaches (**EDBs**);
- 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.

Under the NDB Scheme, any organisation or agency covered by the Privacy Act must notify the OAIC when a data breach is likely to result in serious harm to an individual whose personal information is involved. While there is a mandatory element to the NDB scheme, the OAIC also receives notifications from entities of data breaches which are not EDBs and which are therefore made on a voluntary basis. For example, entities may wish to notify the OAIC where they are unsure of whether a data breach is an EDB, or for guidance and reporting purposes even though:

- the entity is not subject to the Privacy Act (such as state or territory government agencies where the data breach does not involve a tax file number);
- an exception under ss 26WM, 26WM, 26WP or 26WQ of the Privacy Act applies; or

- serious harm is not likely to occur as a result of the data breach (per s 26WE(2)(a)(ii) of the Privacy Act).

Such notifications are still registered as Data Breach Notifications on the OAIC's matter management system, Resolve, and have been included in the document created under s 17 of the FOI Act.

Further, even where an entity is required to report an EDB to the OAIC, the OAIC's NDB form allows for further information to be provided in addition to the information required under the NDB Scheme. The OAIC's NDB form states that:

> *The OAIC encourages entities to provide additional information to assist us in understanding the eligible data breach. Part two of the form is optional… and you may request that it be held in confidence by the OAIC.*
>
> *…*
>
> *The OAIC will respect the confidence of commercially or operationally sensitive information provided voluntarily in support of a data breach notification, and will only disclose this information after consulting with you, and with your agreement or where required by law.*[1]

The OAIC's NDB team has advised that:

- compliance with the NDB Scheme generally relies on good faith of regulated entities, including agencies, to undertake assessments of data breaches and notify the OAIC; and
- notification to the OAIC, and provision of as much information as possible, can enable the OAIC's oversight of the notifying agency's assessment of the incident and whether notification of the incident to individuals ought to occur.

Details of data breaches (columns 5-7)

I have decided that columns 5-7 of the document are exempt under s 47E(d). This information is mandatory where an EDB occurs, however the level of detail contained in these columns (being the date of the data breach, description of the data breach, and kinds of personal information involved) all rely on entities being as forthcoming as possible in providing detail to the OAIC. The OAIC states on its NDB form that it will 'collect this information to consider and respond to your breach notification', and publishes aggregated information in its Notifiable Data Breach Report in order to 'help entities and the public understand privacy risks identified through the scheme, highlight areas that require attention and provide clarity around our regulatory

[1] OAIC Notifiable Data Breach form - for training purposes only

approach.' Generally reporting entities would not expect the details of a data breach to be shared outside of the OAIC and affected individuals.

Some agencies have expressed a particular concern over this information being released in light of the following:

- where agencies are still investigating the full circumstances of a data breach they nonetheless wish to advise the OAIC of what they know at that time, and the initial details provided may be incomplete or inaccurate;
- the level of detail provided in these descriptions may expose them to further data breaches by exposing vulnerabilities in their systems and processes; and
- agencies may voluntarily share more information than is required with the OAIC in the spirit of cooperation and to allow the OAIC to gain valuable insights and better prevent further data breaches, but on the understanding that this information is only for the OAIC's benefit.

While I acknowledge that the completion of these information fields is mandatory (where there is indeed an EDB), I consider that it is reasonably likely that if this information were disclosed, reporting entities would be less detailed and forthcoming in how they disclose this information to the OAIC. I consider that this would substantially adversely affect the OAIC's ability to:

- assess whether the entity has met its obligations under the NDB Scheme, such as notifying affected individuals;
- assess whether further regulatory action is needed in response to the notification (for example, commencement of an investigation under the Privacy Act);
- provide further assistance to affected entities; and
- collect broader information on the causes and impacts of data breaches which is required for the OAIC to provide timely and effective guidance to entities and the public.

Names of agencies and OAIC reference numbers (columns 1 and 3)

I have also decided that some names of agencies and the OAIC reference number associated with the breach are exempt under s 47E(d). This is based upon consultation with the OAIC's NDB team along with the affected agencies. I have decided not to release this information where:

- the agency was not required to notify the OAIC of that particular data breach for one of the reasons noted above on pages 9-10; or
- the agency had requested that non-mandatory information be kept confidential by the OAIC (that information, such as number of affected

individuals, would be linked to the agency due to those columns of the document being released both in the original decision and internal review).

The agencies whose names (and associated OAIC reference numbers) I have found exempt have all objected to release of this information, or otherwise indicated that release of it would affect their willingness to provide information on a voluntary basis to the OAIC in the future.

For the reasons listed above regarding the details of the data breaches, I consider that this would have a substantial adverse effect on the OAIC's ability to administer the NDB Scheme, and I consider this information to be exempt under s 47E(d).

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

My consideration of the public interest test is discussed below.

The public interest test – (section 11A and 11B)

As provided above, I have considered that material within the documents is subject to conditional exemption under section 47E of the FOI Act.

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:

> *6.225 It is not necessary for an issue to be in the interest of the public as a whole. It may be sufficient that the issue is in the interest of a section of the public bounded by geography or another characteristic that depends on the particular situation. An issue of particular 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, I consider the following to be relevant:

- disclosure would promote the objects of the FOI Act, in particular, by informing the community of the Government's operations; and
- disclosure would inform debate on a matter of public importance.

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, however the FOI Guidelines at 6.233 provides a non-exhaustive list of factors against disclosure.

In considering the documents subject to this request, I consider that the following factors do not favour disclosure:

- disclosure could reasonably be expected to prejudice the OAIC's ability to obtain confidential information;
- disclosure could reasonably be expected to prejudice the OAIC's ability to obtain similar information in the future; and
- disclosure could reasonably be expected to prejudice the OAIC's ability to administer the NDB Scheme.

On balance, I consider the public interest factors against disclosure to be more persuasive than the public interest factors favouring disclosure. In weighing up these factors, I have given particular weight to the submissions of agencies who objected to release, being those who had requested that certain information be kept confidential and/or who had reported data breaches on a voluntary basis. Some of the comments from these agencies included:

- 'The [agency name] voluntarily shares more information than is required with the OAIC in the spirit of cooperation and to ensure that the agencies can work together as effectively as possible. We believe that this approach allows the Commonwealth to gain valuable insights and better prevent further data breaches. Additionally, in its notification the [agency name] requested that the OAIC hold the information provided in Part Two of the form in confidence. Where there is a risk that this information may be disclosed publicly, agencies

captured by the notifiable breach scheme may in future only provide strictly required information.'

- '[Agency name] has willingly complied with this advice [to report data breaches that may not be EDBs] and developed a strong relationship with the OAIC. Voluntarily reporting these breaches allows [agency name] to receive valuable advice from the OAIC, and the OAIC to be aware of incidents that are occurring in the agency. This exchange of information and advice is done on the basis of confidentiality. [agency name] was not obliged to report these matters to the OAIC under the Notifiable Data Breaches Scheme.'
- 'Notification of these data breaches were provided to the OAIC on a confidential basis. Disclosure of the details of these notifications, including information that identifies [agency name] as the agency involved could reasonably be expected to have a substantial adverse effect on the proper and efficient conduct of the operations of the OAIC as the quality of data breach reports in the future may be prejudiced. Disclosure could jeopardise the process of provision of such information and, in turn, have a substantial adverse effect on the OAIC's ability to receive similar information in the future. Given that [data breaches] did not result in further action or investigation by the OAIC, disclosure of these entries would be contrary to public interest as it could reasonably be expected to inhibit interagency communications and notifications as it would create a precedent that any and all data breaches, no matter how minor and whether further action was taken or not by the OAIC would be expected to be disclosed to the public.'

Accordingly, based on the information before me at this time, I am satisfied that release of the exempt material would be contrary to the public interest.

Additional information from agencies

In the course of consulting with agencies named in the document, some agencies have provided additional context or information about their reported data breaches included in the report that I note here for your reference.

The Department of Employment and Workplace Relations (**DEWR**) did not object to release of its name but has noted that in the case of both breaches the DEWR's data was accessed by a third party, either maliciously or without authorisation. While the document names the source of DBN22/00677 as 'rogue employee/insider threat' the personal information in question was accessed by an employee of a service provider of DEWR, not by a DEWR employee.

The Commonwealth Scientific and Industrial Research Organisation (**CSIRO**) also did not object to release of its name but did note that the particular matter linked to the

CSIRO (DBN23/00817) was voluntarily reported by the CSIRO. This was a data breach suffered by a service provider and so the CSIRO did not have an obligation to notify the OAIC under s 26WM.

Service NSW has clarified that when they reported DBN20/00480 to the OAIC they did not state the total number of individuals impacted. It was estimated that the number of impacted individuals were approximately 103,000, however the OAIC's reporting reflected in the document captures the OAIC's understanding of the data breach at a point in time as recorded by the OAIC when registering the NDB.

Disclosure log determination

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 documents

The documents and my decision on internal review are identified in the attached schedule of documents.

The documents are enclosed for release.

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

Yours sincerely

Molly Cooke
A/g Senior Lawyer
25 September 2024

If you disagree with my decision

Further Review

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

You have the right to seek review of this decision by the Information Commissioner (IC review). If you wish to apply for IC review, you must do so in writing within 30 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.

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 post your application to:

> Office of the Australian Information Commissioner
> GPO Box 5288
> SYDNEY NSW 2001

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