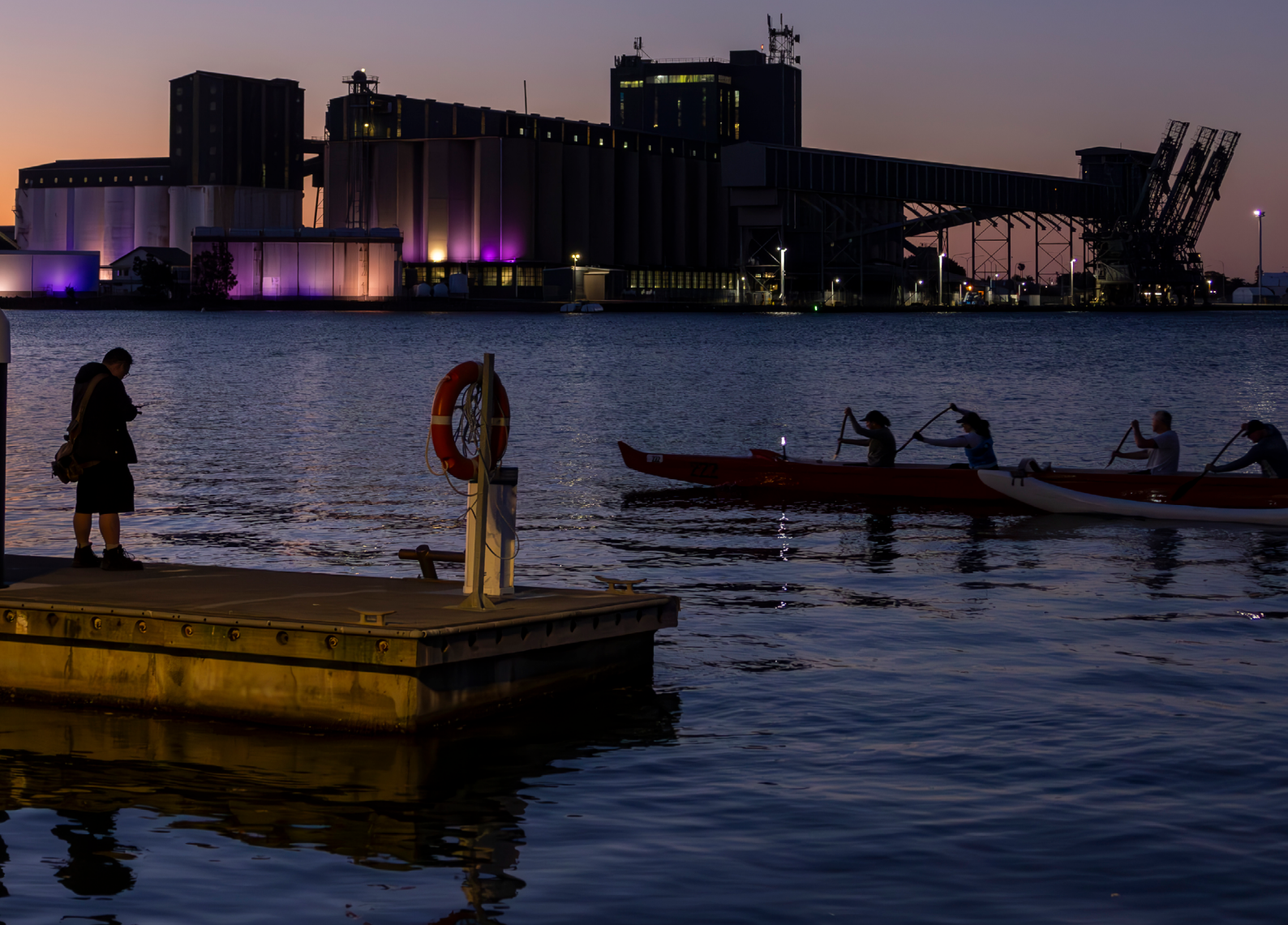
Australian Government

Net Zero Economy Authority

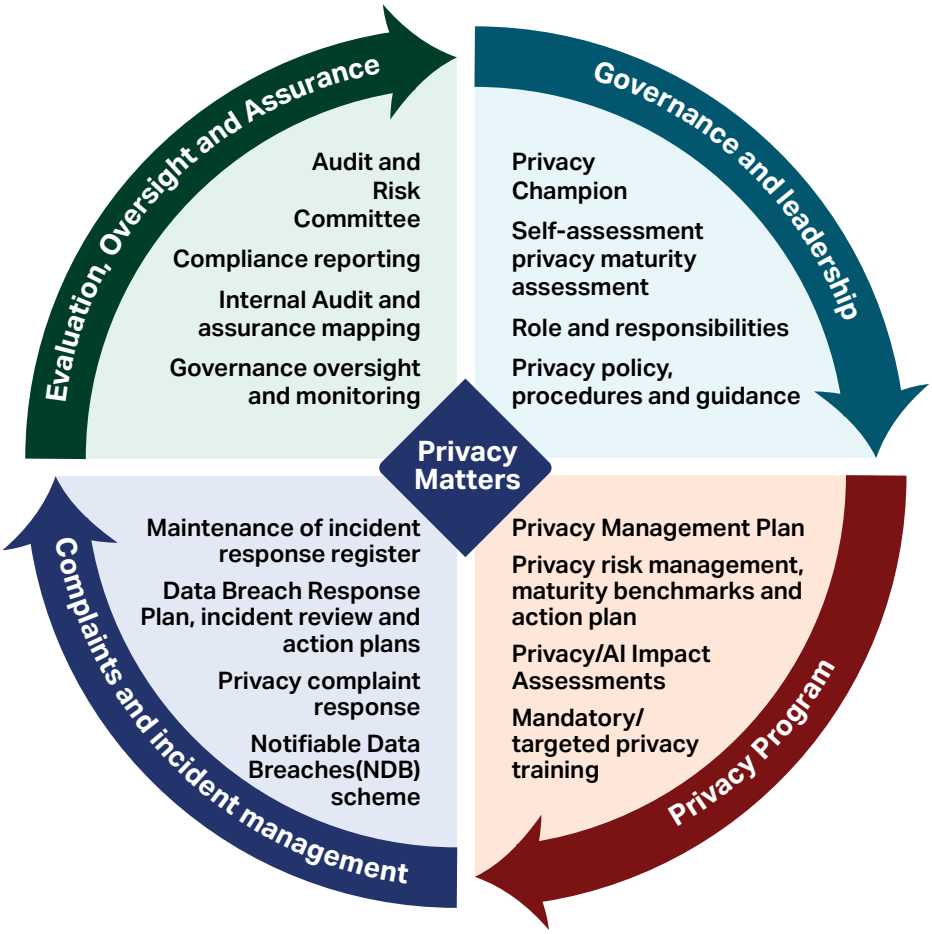
Privacy Policy 2026-2028



Contents

Overview

1. This policy explains the kinds of personal information collected by the Net Zero Economy Authority (the Authority) and why. It outlines how the Authority handles personal information and sensitive information, how staff and others can access or correct personal information and how individuals can contact the Authority to discuss or complain about any concerns they have about the collection, use or disclosure of their personal information.
2. The Authority will review this policy on a biennial basis or following any relevant legislative or policy change to ensure it reflects current laws and addresses the needs of the Authority and staff.



The Authority's obligations in relation to the information

3. The Authority is subject to:
   a. The *Privacy Act 1988* (Cth) (the Privacy Act), the requirements of the Australian Privacy Principles (APPs) at Schedule 1 of the *Privacy Act and the Privacy (Australian Government Agencies - Governance) APP Code 2017* (the Code).
   b. The *Net Zero Economy Authority Act 2024* (Cth) (NZEA Act), as it relates to the Energy Industry Jobs Plan (EIJP).
   c. Obligations under other legislative frameworks to protect personal information, including the *Public Governance, Performance and Accountability Act 2013*, the APS Code of Conduct (s 13 of the *Public Service Act 1999*) and the *Crimes Act 1914*.
   d. The requirements of the *Archives Act 1983* relating to Commonwealth records (including the disposal, alteration and destruction of such records) which applies to the Authority's records, including personal information held by the Authority.
4. The Authority has a Privacy Matters Practical Guide to assist staff with meeting the APP requirements.

Why the Authority collects personal information

5. The Authority collects, uses and discloses *personal information* about its stakeholders, board members and staff in the course of undertaking its roles and functions under the NZEA Act, including:
   a. Performing functions under the NZEA Act and other relevant Australian Government legislative and policy settings.
   b. Facilitating invitations for, and the running of, public submission and consultation processes, including with respect to policy, programs and services the Authority delivers, and the review or reform of policy and processes.
   c. Facilitating invitations to subscription services so that individuals who subscribe can receive information and other communications from the Authority.
   d. Undertaking recruitment and managing employment (including reasonable adjustments, entitlements, remuneration and performance management).
   e. Facilitating travel and security arrangements.
   f. Conducting research the Authority has commissioned or has partnered to deliver.
   g. Coordinating intergovernmental policy matters with States and Territories.
   h. Responding to correspondence from members of the public or organisations to the Authority, the Prime Minister, portfolio Ministers or other Australian Government Ministers and agencies.
   i. Facilitating events, official visits and appointments.
   j. Handling complaints (including privacy complaints) and feedback provided to us.
   k. Administering programs, contracts and grants.
   l. Facilitates interactions and engagements with stakeholders.
6. You can find out more about the Authority's functions on its website.
7. The Authority will not ask for personal information it does not need. The Privacy Act requires that the Authority only collects information for purposes that are reasonably necessary for, or directly related to, the Authority's functions and activities, including to facilitate interactions and engagements with stakeholders.[1]

What Information We Collect

8. ***Personal information*** means information or an opinion about an identified individual, or an individual who is reasonably identifiable.[2]
9. Personal information includes a broad range of information or opinions that could identify an individual. What is personal information will vary depending on the circumstances. The Authority collects different types of personal information depending on the category of individual e.g. staff, the Board and stakeholders. Examples include:
   a. an individual's name
   b. signature
   c. address
   d. telephone number
   e. email address
   f. organisation
   g. position
   h. details of engagements and interactions with the NZEA
   i. date of birth
   j. work history and education (including on a resume)
   k. medical records
   l. bank account details
   m. photos and videos
   n. government identifiers (NZEA staff))

[1] See APP 3.
[2] What is personal information? | OAIC

o. voice print and facial recognition biometrics
p. any additional kinds of information the NZEA may collect in the course of making a grants application (e.g. employment contracts).

10. ***Sensitive information*** is a subset of personal information, and has a higher level of privacy protection than other personal information. The Authority will only collect, use and disclose sensitive information with an individual's permission or where required by law. Sensitive information includes information or an opinion about an individual's:
    a. trade union memberships or associations
    b. racial or ethnic origin
    c. political opinions
    d. religious or philosophical beliefs or affiliations
    e. sexual orientation
    f. criminal record
    g. health or genetic information
    h. some aspects of biometric information.

How the Authority collects personal information

11. The Authority collects personal information through a number of means including through surveys, email and phone communications, correspondence and submissions, forms and notices, through online portals and our website. These means may include the collection of personal information where individuals subscribe to the Authority website to receive updates or interact with the Authority through a Your Say service.
12. The Authority may also collect personal information from:
    a. an individual directly
    b. face to face meetings/phone calls
    c. through the use of the NZEA Customer Relationship Management (CRM) system (including in data logs)
    d. through their authorised representative(s)
    e. via a third party, if permitted by law
    f. correspondence and submissions
    g. paper-based forms
    h. online (website forms, virtual meetings and email).
13. When the Authority collects personal information it will:
    a. notify individuals through a privacy collection notice (PCN), if it is reasonable to do so. The notice will include reasons why the Authority is collecting the information, whether the collection is required or authorised by law, and any person or body to whom the Authority usually discloses the information. Where information is to be shared with other government agencies, a PCN will include why the information is being shared with the other agencies, if it is reasonable to do so.
    b. inform individuals how they can request access to, or correction of, their personal information, and who to contact if they have a privacy enquiry or wish to make a complaint.
14. In some situations, the Authority may not be able to notify individuals through a PCN, for example when:
    a. notification would be inconsistent with another legal obligation, for example, by breaching a statutory secrecy provision, a client's legal professional privilege, or a legal obligation of confidence, or
    b. notification may pose a serious threat to the life, health or safety of an individual or pose a threat to public health or safety, for example, a law enforcement agency obtaining personal information from a confidential source for the purpose of an investigation.
15. Where the Authority collects person information about employees from employers or organisations, the Authority must take steps to confirm that the employer or organisation has received consent from the individual to share their personal information with the Authority prior to the collection.

16. For grants applications, personal information will be sought through an online application form via the Grants Hub operated by the Department of Industry, Science and Resources (DISR). An agreement for sharing this information between the DISR and the Authority is being prepared. The information held by DISR and shared through this agreement will be treated in accordance with the Privacy Act and the APPs. An applicant acknowledgement for the collection of personal information will be included in the application form.

Anonymity, pseudonyms and uncollected information

17. In some circumstances individuals may have to provide personal information. For example, the Authority may require personal information to assess an individual's eligibility for a program or service or confirm their identity for release of personal information.
18. Individuals are able to use a pseudonym or remain anonymous when interacting with the Authority, however there will be circumstances where that will not be practicable, such as for:
    a. the Energy Industry Jobs Plan, and
    b. employment opportunities at the Authority.
19. The Authority will advise individuals if they are, or are not, able to remain anonymous or use a pseudonym when dealing with the Authority.
20. The Authority will also advise that it will be unable to engage with individuals if all necessary personal information is not provided. For the CRM, personal information will need to be collected to facilitate and record interactions between the Authority and individuals. If the information is not collected, the Authority will not be able to manage interactions between the Authority and individuals and organisations. That includes, potentially, with respect to access to the Online Jobs Portal.

Collecting information through the Authority website

21. To improve visitor experience to the Authority's website, the Authority may use 'cookies'. Cookies enable a website to remember an individual's use of the website either for the duration of the visit or for repeat visits.
22. The Authority's website is hosted in Australia but uses Google Analytics, which transmits website traffic data to Google servers in the United States. Google Analytics does not identify individual users or associate an individual's IP address with any other data held by Google. The Authority uses reports provided by Google Analytics to help it understand website traffic and webpage usage in order to improve user interaction with the website.
23. By using the Authority's website, individuals consent to the processing of data about them by Google in the manner described in Google's Privacy Policy and for the purposes set out above. **However, individuals can opt out of Google Analytics if they disable or refuse the cookie, disable JavaScript, or use the opt-out service provided by Google**.
24. The Authority's website may also contain links to other websites, **however the Authority is not responsible for the content or privacy practices of other linked websites**. Individuals using websites linked to the Authority's website are advised to be aware and read the privacy policies of those respective websites. Find out more about the Authority's collection and use of information from its websites and social media platforms in our Website and Online Communications Privacy Collection Notice.

How the Authority holds and safeguards personal information

25. The Authority takes seriously its obligations to protect the personal information it holds, including taking reasonable steps to protect personal information against misuse, interference and loss, and from unauthorised access, modification or disclosure. These steps include:
    a. Classifying and storing records securely in accordance with Australian government security and records management policy settings.[3] All information will be held as an electronic record. Further, the CRM involves holding personal information in Microsoft Azure, a cloud-based application. All records of stakeholder interactions will be stored in the CRM.
    b. Only personnel with a strict 'need to know' basis will have internal access to information.
    c. Monitoring system access with controls and authenticated credentials.

[3] Australian Government Protective Security Policy Framework, Information Security Manual, APPs.

d. Ensuring our buildings are secure.
e. Regularly updating and auditing our storage and data security systems.

26. When personal information is collected through a third party, such as a contracted service provider (CSP), the Authority will inform the third party about its privacy practices, and, where suitable, also inform impacted individuals of the collection. This may also occur through this Privacy Policy, notices or discussions with Authority staff. The Authority will require CSPs not to do an act, or engage in a practice, that would breach an APP.
27. Where personal information is no longer required, the Authority will archive, de-identify or dispose of the records in accordance with the *Archives Act 1983* and normal administrative practice policy or applicable records disposal authorities. Further guidance on archiving, de-identifying, destruction and disposal of records is available in the Practical Guide.

Data Breach Response Plan

28. If personal information held by the Authority is lost or subject to unauthorised access or disclosure, the Authority's response will comply with:
    a. the Office of the Australian Information Commissioner's Data breach preparation and response — a guide to managing data breaches in accordance with the Privacy Act, and
    b. the Authority's Data Breach Response Plan.
29. If a data breach is likely to result in serious harm[4] to individuals, the Authority's response will include providing timely advice to affected individuals.
30. If the Authority receives unsolicited personal information, the Authority will assess whether it could have lawfully collected the information as if it had solicited it.[5] Additional information on how to deal with unsolicited personal information is available in the Practical Guide.
31. If a determination cannot be made as to whether the personal information was lawfully collected and subject to any exception under s 24 of the *Archives Act 1983*, the Authority will destroy or de-identify the information.[6]

How the Authority uses and discloses personal information

32. With the exception of government related identifiers, APP 6[7] permits the Authority to use and disclose collected personal information for the primary purpose of its collection. The Authority will take reasonable steps to inform individuals about the reason for collection at the time of the collection, or as soon as practicable thereafter.
33. The Authority may also use and disclose the information for a 'secondary purpose' in particular circumstances, including when:
    a. Individuals consent to disclosure
    b. Individuals would reasonably expect the Authority to use or disclose the information for the secondary purpose
    c. The secondary use or disclosure is required or authorised by or under an Australian law or a court/tribunal order
    d. A permitted general situation exists in relation to the use or disclosure of the information by the Authority
    e. The Authority believes the secondary disclosure is reasonably necessary for enforcement-related activities
    f. The Authority participates in merit or judicial review proceedings in tribunals or courts or institutes proceedings in courts, or
    g. The information is biometric information, or biometric templates, to be disclosed to an enforcement body in accordance with guidelines made by the Information Commissioner for these purposes.

[4] 'Serious harm' is not defined in the Privacy Act. In the context of a data breach, serious harm to an individual may include serious physical, psychological, emotional, financial, or reputational harm.
[5] See APP 3 and 4.
[6] Except where the information is contained in a Commonwealth record or if it is not reasonable and lawful to destroy or de-identify.
[7] APP 6 outlines when the Authority may use or disclose personal information. The intent is that the Authority will generally use and disclose an individual's personal information only in ways the individual is aware, has consented, would expect or if required by law or a court/tribunal order.

34. The Authority may disclose personal information to overseas third parties (such as a foreign government or agency) where this is a necessary part of the Authority's work. Such disclosure to overseas third parties will only occur when:
    a. Individuals have consented to the Authority disclosing personal information to that third party.
    b. The Authority reasonably believes that:
        i. the overseas recipient is subject to a law or binding scheme that is, overall, substantially similar to the APPs, and
        ii. the law or binding scheme can be enforced; or
    c. The disclosure is required or authorised by an Australian law or court/tribunal order.
35. The Authority may also use third party providers to deliver or otherwise communicate content. These third parties, which may collect and store your personal information in servers outside of Australia, may include: Google, Facebook, X (formerly Twitter), Campaign Monitor, LinkedIn, Instagram, YouTube and others.
36. Such third-party sites have their own privacy policies and may send their own cookies to an individual's computer. As noted earlier, the Authority does not control the setting of third-party cookies and recommends that individuals check the third-party websites for more information about their cookies and how to manage them.
37. The Authority will only use or disclose a government related identifier where permitted by APP 9.2.
38. The Authority will only use or disclose personal information for direct marketing where an individual has either consented to or would reasonably expect that use or disclosure. Individuals will be able to opt out of receiving direct marketing communications.
39. To opt out of direct marketing, an individual can click the unsubscribe link at the bottom of the communications or by emailing the Authority Privacy officer at NZEA-Privacy@pmc.gov.au.
40. Personal information should not be shared or disclosed other than as described in this privacy policy unless:
    a. The individual has provided explicit consent
    b. The disclosure is authorised or required by or under an Australian law or court/tribunal order, or
    c. Is otherwise permitted under the Privacy Act.

Specific information regarding the Energy Industry Jobs Plan [8] (EIJP)

41. The Authority may collect personal information for the EIJP in several ways, including:
    a. During public consultation and the collection of written submissions through Community of Interest (COI) processes.
    b. When information is voluntarily disclosed to help the Authority determine if an EIJP is needed.
    c. Following a notice from the CEO to provide information under s 64 of the NZEA Act.
    d. When an individual opts in to become a participating employee under the EIJP.
    e. Monitoring employers' compliance with ss 58, 59, 60, 61 and 62, per s 68 of the NZEA Act.
42. In accordance with the objects of the NZEA Act and Part 5 specifically, personal information may be collected for the purposes of assessing and implementing an EIJP. This information may include:
    a. The names of 'transition employees' and 'participating employees' of closing or dependent employers.
    b. Contact details for those employees.
    c. Equity and diversity characteristics for those employees.
    d. Employment details for those employees.
    e. The occupations, qualifications, training and skill sets of those employees.
    f. Personal opinions about, or information that relates to, a particular power station closure being assessed under the EIJP.
43. While the Authority may collect this information, it will be limited to what information is needed and authorised by law.

[8] As governed by Part 5 of the NZEA Act.

44. The Authority may identify dependent employers not only under s 6 of the Act through consultation conducted in line with s 55 of the Act, but also using information from a range of sources, including but not limited to closing employers, publicly available data, and government-held records.
45. Personal information collected for the EIJP is for that purpose only and is not authorised for use for any other purpose, unless otherwise consented to by the individual.
46. For consent to be valid, it must have the following four elements:
    a. Voluntary: The individual has a genuine opportunity to provide or withhold consent.
    b. Informed: The individual properly and clearly informed of the implications of providing or withholding consent.
    c. Current and Specific: Consent is sought for a fixed period (not indefinitely) and for specific purposes (rather than bundled into one consent).
    d. Capacity: The individual has the ability to understand the nature of the decision, form a view and communicate that decision.
47. The Authority will only collect personal information it needs to perform its duties and functions.
48. The Authority may disclose collected personal information:
    a. By publishing non-confidential submissions on the NZEA website. All personal information will be removed before publication, unless explicit consent is given.
    b. To the Fair Work Commission (FWC) as part of the COI process in accordance with the Privacy Act. A PCN will be provided to individuals which details of the collection, use and disclosure of information.
    c. When required and consented to by the individual, relevant personal information to stakeholders involved in the COI process, such as receiving employers, closing and dependent employers, and employee and employer organisations.
    d. By disclosing de-identified data to other federal or state government entities to inform policy development and evaluation.
49. In all instances where the Authority discloses an individual's personal information to potential future employers or others, it will take the necessary steps to inform the recipient of the nature of the information provided to ensure the individual's personal and sensitive information remains protected.
50. An individual's employer is required by subparagraph 58(1)(ba) of the NZEA Act to inform them that if they opt in as a participating employee, their personal information may be given to the CEO of the Authority under s 64 and disclosed under s 66 of that Act. The Authority may disclose a participating employee's personal information to potential future employers for employment consideration. The Authority will provide a way for individuals to specify which employers they do not want their information shared with, if any.
51. Individuals can make submissions during a COI process anonymously or by using a pseudonym. However, if an individual chooses this option, the Authority may not be able to verify or clarify the information received, which could impact how the submission is considered. Any submission made to the Authority for the EIJP may also be subject to a request under the *Freedom of Information Act 1982* (Cth) (FOI Act).
52. As far as possible, the Authority will minimise the collection of sensitive information. For example, in the event of follow-up requests that may require more granular information, the Authority will advise the reasons for seeking additional information.
53. The Authority will require employers to confirm that their response does not include personal/sensitive information by including words like "by submitting this form you confirm that you have not included any personal/sensitive information, other than contact details for representatives of potential dependent employers."
54. Generally, the Authority does not expressly request sensitive information. An individual may choose to supply sensitive information where relevant in a job-application or worker re-redeployment form.
55. However, we may require employers to provide aggregate sensitive information about employees as part of an EIJP consultation process. In circumstances where the Authority uses forms to request sensitive information, such as for a job application or in worker redeployment forms, it will be optional for individuals to provide this information.

56. When an individual opts in to become a participating employee under the EIJP, the Authority may also collect personal information to fulfil its EIJP obligations under Part 5 of the NZEA Act.

Accessing, correcting and deleting personal information

57. Individuals have the right to request access to personal information which the Authority holds about them, and to request that information be corrected if they believe it may be incorrect. Individuals (or their authorised representative) can make such a request by phone, email or letter to the Authority.
58. The Authority will aim to address such requests within 30 days, and where possible, will provide written confirmation of the outcome. However, the Authority will not provide access to an individual's personal information without first verifying their identity or their representative's authority to make the request.
59. In certain circumstances under the Privacy Act, the Authority can refuse access to an individual's personal information, including where an exemption under the *Freedom of Information Act 1982* (FOI Act) would apply.
60. If the Authority refuses access, it will provide reasons in writing for doing so, together with information about options for disputing or challenging the Authority's decision.
61. The Authority will take reasonable steps to correct the accuracy of personal information to ensure that, considering the purpose it is held for, it is accurate, up-to-date, complete, relevant and not misleading. If the Authority has received personal information from a third party, the Authority will advise the third party of any corrections made to that information.
62. Even if individuals do not ask the Authority to correct personal information, the Authority is required to take such steps (if any) that are reasonable in the circumstances, to correct personal information if it is satisfied that, having regard to the purpose for which the information is held, the information is inaccurate, out-of-date, incomplete, irrelevant or misleading.
63. If the Authority refuses a request to correct personal information, it will provide its reasons for doing so and will also provide advice about complaints mechanisms available in relation to that refusal.
64. The Authority may be able to delete an individual's personal information in certain circumstances, for example if the personal information:
    a. Is no longer required for the Authority's functions or activities
    b. Is not contained in a Commonwealth record for the purposes of the *Archives Act 1983*, or
    c. Is not required to be held under other legislation.

Privacy Management Plan

65. A Privacy Management Plan (PMP) identifies specific, measurable goals and targets, and sets out how an agency will meet its compliance obligations under APP 1.2. The *Privacy (Australian Government Agencies – Governance) APP Code 2017* (Cth) (the Privacy Code) requires agencies to have a PMP and to measure and document performance against the plan at least annually. The Authority's PMP outlines the actions the Authority will be taking within a 12-month period to ensure compliance with APP 1.2.

Privacy Impact Assessments

66. The Privacy Code requires the Authority to conduct a Privacy Impact Assessment (PIA) for all high privacy risk projects.
67. A PIA is a systematic assessment of a project that identifies potential privacy impacts and recommendations to manage, minimise or eliminate them.
68. To be effective, a PIA should be an integral part of the project planning process; it can help facilitate a privacy by design approach, identify better practice, and help ensure compliance with the Privacy Act. Australian Government agencies are also required to undertake a PIA for all privacy risk projects.
69. The Authority must publish a PIA register on our website pursuant to section 15(1) of the Privacy (Australian Government Agencies- Governance) APP Code 2017, made under the Privacy Act.

Contacting the Authority about your personal information

70. In the first instance, an individual seeking to request access to, correction of, or deletion of their personal information may contact the Authority's Privacy Officer (contact details below), for guidance about the request, including whether the request is best dealt with under the Privacy Act, the FOI Act or other process.

    Email: Privacy Officer

    Post: Privacy Officer
    Net Zero Economy Authority
    PO Box 1267
    CANBERRA ACT 2600

71. In particular, individuals should contact the Privacy Officer if they would like:
    a. to ask questions about the Authority's privacy policy
    b. a copy of this policy in an alternative format
    c. access to or correction of that person's personal information held by the Authority, or
    d. to make a complaint.

Making a complaint to the Authority

72. If an individual is not satisfied with how the Authority has collected, held, used or disclosed their personal information, they can make a formal complaint to the Authority's Privacy Officer.

73. The complaint should include:
    a. A short description of the privacy concern.
    b. Any actions or dealings the individual or their representative has had with Authority staff in relation to the privacy concern.
    c. Preferred contact details so the Authority can provide a response to the complaint.

74. If an individual is not satisfied with the Authority's response to or resolution of the complaint, they may lodge a further complaint with the Office of the Australian Information Commissioner (OAIC).

75. The OAIC can receive privacy complaints through:
    a. The online Privacy Complaint form (refer to the OAIC's website)
    b. By email (Note: email that is not encrypted can be copied or tracked) at enquiries@oaic.gov.au
    c. By mail (or registered mail if there are concerns about the confidentiality of information sent via the post) to:

    Office of the Australian Information Commissioner
    Sydney Offices
    GPO Box 5218
    Sydney NSW 2001