elevenM

Office of the Australian Information Commissioner

Web Analytics

Privacy Impact Assessment

Final

25 September 2025

elevenM Consulting Pty Ltd ABN 77 610 787 534

Contents

Document control

Version	Date	Comments	Author
0.1	18/07/2025	Initial draft	elevenM
1.0	25/09/2025	Final (minor clarifications on findings)	elevenM

Executive summary

Background

The Office of the Australian Privacy Commissioner (**OAIC**) has engaged elevenM to undertake a privacy impact assessment (**PIA**) of the web analytics implementation on its website at https://www.oaic.gov.au/ (**website**). This assessment covers:

- the existing Google Analytics 4 (**GA4**) implementation and configuration
- web analytics data collection facilitated through Google Tag Manager (**GTM**).

Findings

This assessment has identified no compliance risks associated with the OAIC's current implementation of GA4. The configuration reflects a low-risk approach to web analytics, with minimal data collection settings, strong access controls, and appropriate transparency measures.

While no compliance recommendations have been made, two best practice recommendations are provided in this report to further enhance user transparency and align with community expectations.

BEST PRACTICE REC. 1 Publish a dedicated web analytics notice that outlines the types of data collected, the purpose of collection, and how users can manage or opt out of tracking.

BEST PRACTICE REC. 2 Update the website's cookie banner to include more specific information about web analytics data collection and provide direct links to relevant privacy information and user control options.

Next steps

The OAIC (in conjunction with other stakeholders) should:

1. Consider and respond in writing, at a senior management level, to the findings outlined in this document.
2. Ensure that any risks identified in this document are recorded and managed according to its risk management framework.
3. Consider publishing this PIA (or a summary of it) on its website or otherwise making its findings publicly available.

Introduction

Background

The OAIC has recently implemented GA4 to gain more detailed insights into how users interact with its website. This upgrade is part of a broader strategy to enhance user engagement, improve digital service delivery, and support organisational efficiency.

To ensure that the integration of GA4 aligns with privacy obligations and community expectations, the OAIC has internally conducted a PIA which focussed on how web analytics data is collected, used, and managed, and considered the potential privacy impacts on users.

The OAIC has subsequently commissioned this external PIA. This document aims to assess potential privacy risks associated with the adoption of GA4 and to provide recommendations that ensure compliance with relevant privacy obligations and best practices.

About GA4

The OAIC's website team currently oversees the implementation and ongoing management of GA4.

GA4 is integrated with the OAIC's website to collected and process web analytics to provide key metrics on web traffic, click-through rates, time spent on pages, downloads, and other user behaviours. Insights from the collected metrics are used to produce reports which are used by the website team to optimise the user journey and improve the overall website experience.

At this stage, the information collected via GA4 includes:

- device IP address (collected and stored in an anonymized format)
- search terms and pages visited on the OAIC website
- date and time when pages were accessed
- downloads, time spent on page and bounce rate
- referring domain and out link if applicable
- device type, operating system and browser information
- device screen size
- geographic location (city).

Geographic location information is limited to country and city level, with no street addresses, latitudes or longitudes collected from users.

GTM is used to manage and deploy tracking codes on the website. GTM acts as a container that controls when and how data collection scripts execute, allowing the OAIC to configure which analytics data is captured without requiring direct code changes to the website.

The OAIC has configured its GA4 implementation with minimal data collection settings, meaning that only the essential metrics outlined above are being collected from website visitors.

De-identification of data

The OAIC has advised that Google processes the information collected via GA4 to remove directly identifying elements before it becomes accessible to the OAIC. This processing includes IP address truncation and the removal of other directly identifying information.

When Google Analytics is implemented, a JavaScript tracking code is deployed on each page of the website. This code collects data on user interactions based on the configuration settings established by the OAIC.

Google processed the collected data to remove directly identifying elements before transferring it to US-based cloud servers. Specifically, IP addresses are truncated[1] so that full IP addresses are not stored in GA4 reports and are not accessible to the OAIC's website team.

GA4 dashboard

The OAIC's website team accesses analytics data through the GA4 interface and reporting dashboards (**Attachment 1:** GA4 dashboard reports). These dashboards are used to analyse website performance data and generate insights for internal stakeholders only.

Strict access controls are enforced to safeguard data within GA4. All access to the platform is browser-based and managed exclusively by OAIC's website team. Access to dashboards and analytics data is granted on a need-to-know basis, with detailed logs maintained to monitor all user activity.

Any changes to user access permissions are recorded within GA4's audit logs. Login credentials are not shared under any circumstances, and access details will be regularly reviewed and updated – particularly when team members leave the organisation – to ensure continued security and accountability.

Analytics data in the GA4 dashboard is retained for 2 months after which reports are automatically purged from the accessible interface.

Cookies and unique identifiers

GA4 uses cookies and similar tracking technologies to assign unique identifiers to website visitors. These identifiers enable the tracking of user sessions and behaviour patterns across the website.

The OAIC's privacy policy includes information on how web analytics data is collected and managed through Google Analytics (without referring specifically to GA4). The privacy policy

[1] [UA] IP masking in Universal Analytics [Legacy] - Analytics Help

contains two separate sections addressing cookies, including guidance on how users can disable cookies through their browser settings.

Upon visiting the website, users are presented with a pop-up banner that informs them about the use of cookies and provides a link to the privacy policy.

Scope

This PIA considers the privacy impacts of implementing GA4 on individuals, specifically focussing on privacy compliance obligations and reputational risks, and makes recommendations to address identified risks.

This document represents a holistic consideration of the practical privacy impacts of implementing and using GA4 and is not legal advice.

Any differences between the design of this activity reflected in this document and the final design as deployed should be considered in a new or updated PIA.

In scope

This PIA considers the risks that, in implementing and operating GA4, the OAIC may not comply with the *Privacy Act 1988* (Cth) (**Privacy Act**) and the 13 Australian Privacy Principles (**APPs**) set out in Schedule 1 of the Privacy Act.

This PIA is intended to meet all requirements under the *Privacy (Australian Government Agencies – Governance) APP Code 2017* (Cth) (**Privacy Code**).

Out of scope

This PIA does not consider:

- the OAIC's existing privacy practices, except to the extent that GA4 implementation may impact them
- technical security controls for GA4
- the privacy or security capabilities of third parties that interact with GA4
- compliance requirements arising under legislation other than the Privacy Act and the Privacy Code
- any public consultation carried out in relation to the project, and any related reputational privacy concerns.

We have assumed that the OAIC has existing programs to ensure general agency-wide compliance with the Privacy Act.

Methodology

Information gathering

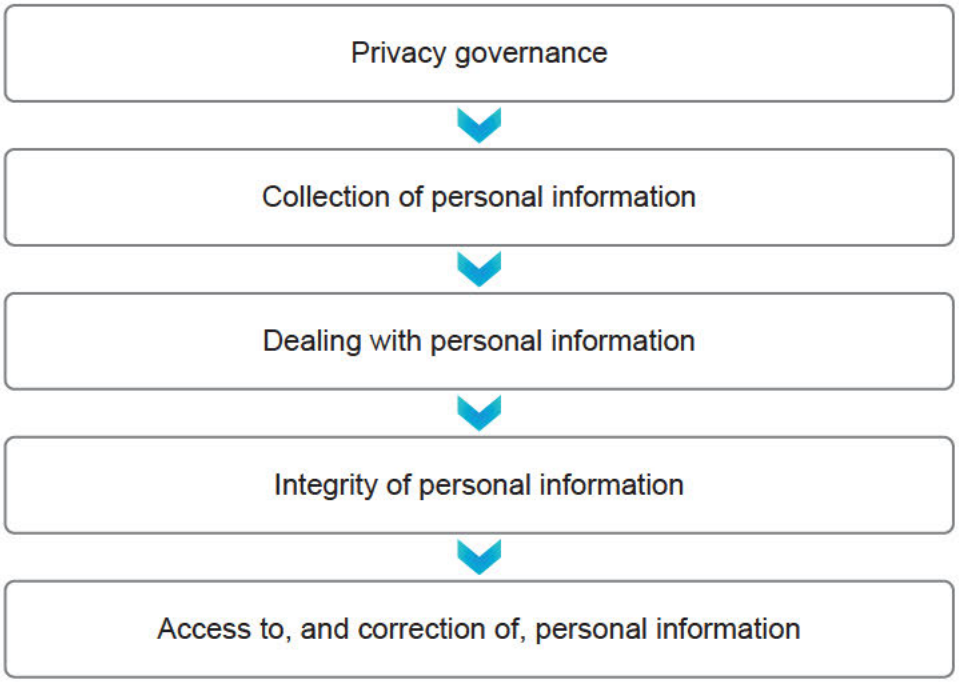
This analysis relies on information gathered through:

- written responses to questionnaires completed by the OAIC
- consultation meetings with OAIC personnel
- review of publicly available materials.

These sources are detailed in **Attachment 2**: Information gathering interviews & materials.

Structure of analysis

The analysis of privacy impacts is organised by reference to the information lifecycle illustrated below:

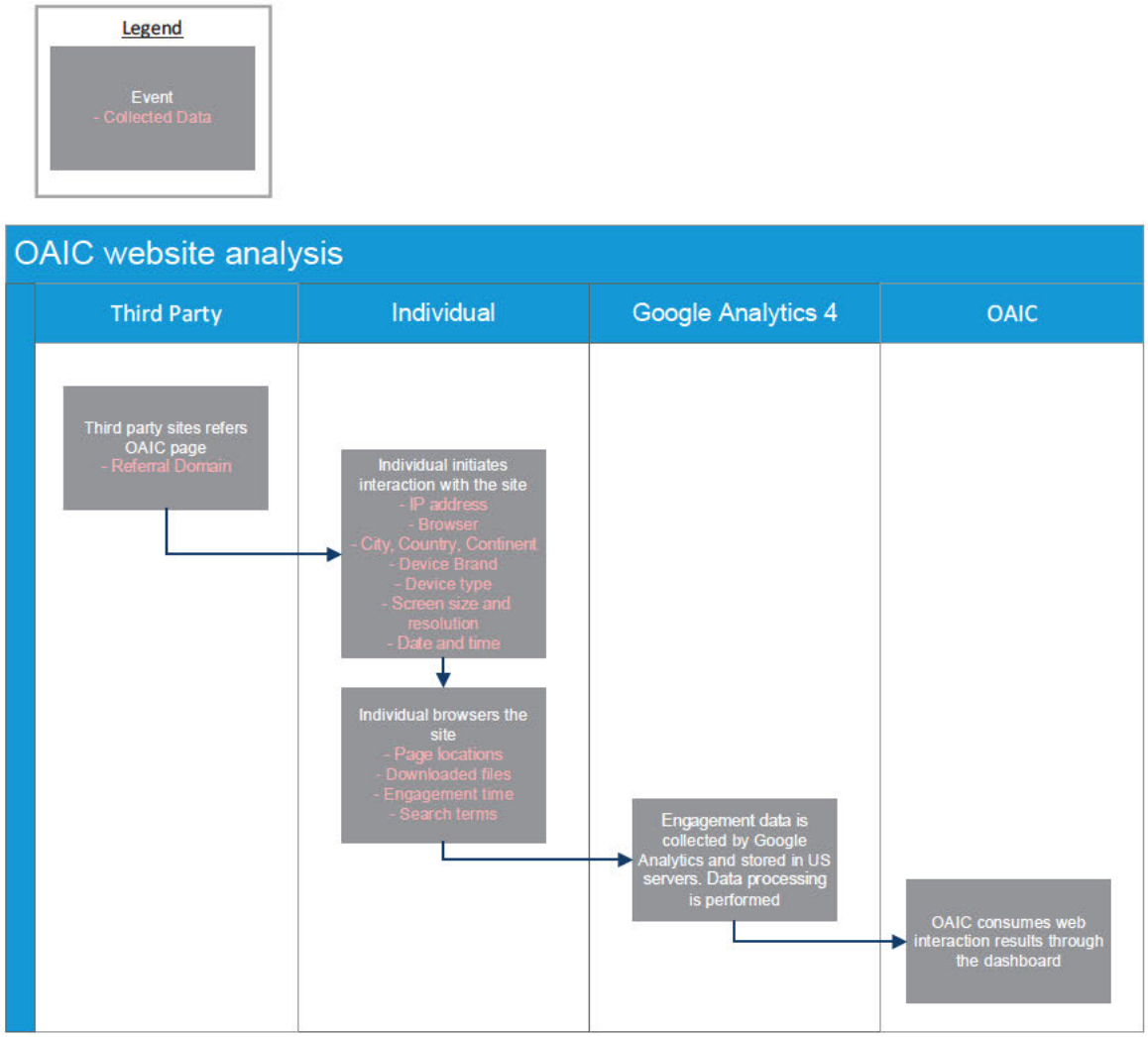


Each stage of the information lifecycle is addressed in a separate section of the analysis. Each section provides a summary of the relevant privacy compliance obligations as they relate to how the implementation of GA4 involves handling personal information, and detailed commentary on whether those obligations are being met.

Where a specific recommendation is classified as '**Compliance**', it indicates that this item alone may constitute a compliance gap and action should be prioritised. However, even findings classified as '**Best practice**' have significance as they are aspects of privacy management and may constitute 'reasonable steps' under APP 1.2.

Information flows

The flow of information between entities is depicted in the diagram below.



Privacy compliance analysis

1. Privacy governance

1.1. Open and transparent management of personal information

APP 1 requires the OAIC to manage personal information in an open and transparent way. This includes having a clearly expressed and up to date APP privacy policy.

Source	Summary of Principle	Analysis
APP 1.2(a)	The OAIC must manage personal information in an open and transparent way. The OAIC must take reasonable steps to ensure it complies with the APPs and must otherwise comply with its obligations under the Privacy Act.	The OAIC's privacy policy addresses web analytics data collection practices, providing transparency about GA4 implementation. The website's cookie notification banner informs users about data collection. Other privacy management obligations, under APP 1.2(a) are outside the scope of this assessment. No relevant findings.
APP 1.2(b)	The OAIC must take reasonable steps to enable it to handle privacy inquiries or complaints.	Privacy inquiry and complaint handling mechanisms are outside the scope of this web analytics assessment. No relevant findings.

Source	Summary of Principle	Analysis
APP 1.3	The OAIC must have a clearly expressed and up to date privacy policy.	The OAIC's privacy policy addresses web analytics data collection. Broader privacy policy requirements are outside scope. No relevant findings.
APP 1.4	The OAIC must ensure that its privacy policy contains specific information set out under APP1.4.	The OAIC's privacy policy includes information about web analytics data collection practices. Other privacy policy content requirements are outside scope. No relevant findings.
APPs 1.5, 1.6	The OAIC must make its privacy policy free, publicly available and in an accessible form.	The OAIC's privacy policy is freely available on its website in accessible format. No relevant findings.
Privacy Code s 16	The OAIC must carry out appropriate privacy training on induction of new staff, and annually where reasonable.	Privacy training requirements are outside the scope of this web analytics assessment. No relevant findings.
Privacy Code s 17	The OAIC must regularly review and update its privacy practices, procedures and systems to ensure that they are current and adequately address the requirements of the APPs. The OAIC must monitor compliance with its privacy practices, procedures and systems regularly.	Privacy practice review requirements are outside the scope of this web analytics assessment. No relevant findings.

1.2. Anonymity and pseudonymity

APP 2 requires OAIC to give individuals the option of not identifying themselves, or of using a pseudonym (subject to limited exceptions).

Source	Summary of Principle	Analysis
APP 2	The OAIC must allow individuals to be anonymous or pseudonymous, except if: • OAIC has legal reasons for not doing so; or • it would impracticable for the OAIC to do so.	Website visitors can access the OAIC website and browse content without providing identifying information or creating accounts. The web analytics data collection through GA4 does not require individuals to identify themselves. Users maintain the option to browse anonymously. No relevant findings.

2. Collection of personal information

2.1. Solicited personal information

APP 3 outlines when OAIC can collect personal information that is solicited. Higher standards apply to the collection of sensitive information.

Source	Summary of Principle	Analysis
APPs 3.1, 3.3, 3.4	The OAIC must only collect personal information and sensitive information that is reasonably necessary for, or directly related to, its functions or activities. The OAIC must obtain consent from an individual, or ensure that an exemption applies under APP 3.4, before it collects sensitive information about that individual.	The OAIC does not directly collect personal information from website visitors via GA4. However, GA4 assigns unique identifiers to browsers and collects associated behavioural data including pages visited, search terms, time spent, device information, and geographic location (city level). Whether this constitutes collection of personal information depends on whether unique identifiers combined with behavioural patterns could reasonably identify individuals. This assessment requires consideration of re-identification risks, which should be evaluated based on the specific data elements collected and technical controls implemented. Under the Privacy Act, information is "personal information" if it is about an identified individual or an individual who is reasonably identifiable. The OAIC's guidance states that whether an individual is "reasonably identifiable" depends on "whether it is possible for the individual or entity that holds the information to identify the individual, using available resources

Source	Summary of Principle	Analysis
		(including other information available to that individual or entity)."[2] The OAIC further notes that "Even though it may be technically possible to identify an individual from information, if doing so is so impractical that there is almost no likelihood of it occurring, the information would not generally be regarded as personal information."[3] Several factors indicate a low likelihood that individuals could be reasonably identified from the collected data: • IP addresses are truncated before storage, removing the most direct identifier • Geographic data is limited to city level only • No names, email addresses, or other direct identifiers are collected • Data is aggregated for reporting purposes • Dashboard access is limited to 2-month retention periods However, certain aspects of the data collection may increase the potential for individuals to be identified:

[2] https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-b-key-concepts
[3] https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/handling-personal-information/de-identification-and-the-privacy-act

Source	Summary of Principle	Analysis
		• Unique browser identifiers persist across sessions and can create detailed behavioural profiles • Search terms may reveal specific interests or personal circumstances • Combination of device characteristics, location, and browsing patterns could potentially distinguish individuals, particularly for users with unique browsing behaviours • Small population centres may make city-level location more identifying Based on the current GA4 implementation with minimal data collection settings, IP truncation, and aggregated reporting, the likelihood that individuals are reasonably identifiable appears low under the OAIC's practical tests. While the combination of persistent identifiers with behavioural data creates some theoretical risk, the technical controls and limited data collection approach significantly mitigate this risk. This assessment recognises this low-level risk and ensures that appropriate technical controls (such as IP truncation, data aggregation, and retention limits) and transparency measures (through privacy policy disclosure and user notification) provide proportionate protections. The data collection remains reasonably necessary for the OAIC's function of optimising website performance and user experience.

Source	Summary of Principle	Analysis
APP 3.5	The OAIC must only collect personal information by lawful and fair means.	The collection of web analytics data through GA4 occurs through standard, transparent web technologies. Users are notified of data collection through the privacy policy and website banner. The collection methods are lawful and fair. No relevant findings.
APP 3.6	The OAIC must collect personal information directly from the individual it is about, unless: • the individual has consented to the personal information being collected from a third party; • OAIC is legally required to collect the personal information from a third party; or • it would impracticable for OAIC to collect the personal information directly from the individual.	Web analytics data is collected by Google through GA4 on behalf of the OAIC, rather than being collected directly by the OAIC from website visitors. However, as assessed above, the data is unlikely to constitute personal information due to the technical controls in place (IP truncation, aggregated reporting, minimal data collection settings). To the extent that any personal information might be collected indirectly, this would fall under the "impracticable" exception in APP 3.6, as it would be impracticable for the OAIC to directly collect detailed web analytics data from each individual website visitor through direct means such as surveys or forms. Users are notified of the data collection arrangement through the privacy policy and website banner. No relevant findings.

2.2. Unsolicited personal information

Source	Summary of Principle	Analysis
APPs 4.1, 4.2	If the OAIC receives unsolicited personal information, it must determine whether it could have collected the information under APP 3. If not, it must destroy or de-identify the information as soon as practicable.	The OAIC has configured GA4 with minimal data collection settings to collect only essential web analytics metrics. The data collected is solicited and necessary for website optimisation purposes. No relevant findings.

2.3. Notification of collection

APP 5 outlines when and how OAIC must notify an individual that it has collected personal information about them.

Source	Summary of Principle	Analysis
APP 5	When it collects personal information about an individual, or as soon as practicable afterward, OAIC must take reasonable steps to notify the individual of relevant matters.[4]	While the web analytics data is unlikely to constitute personal information based on the assessment above, APP 5, transparency about data collection practices supports user trust and aligns with community expectations. The current website banner states "We use cookies to analyse traffic and to improve your browsing experience on our website. To find out more, read our privacy policy." This provides basic notification but does not specifically address web analytics data collection or user control options. The privacy

[4] Relevant matters are set out in APP 5.2.

	policy includes more detailed information about web analytics practices, but this information could be made more accessible to users. Enhanced transparency would represent best practice for a privacy regulator, even where strict compliance requirements may not apply. **BEST PRACTICE REC. 1** Consider developing and publishing a dedicated web analytics notice that outlines the types of data collected, the purpose of collection, and how users can manage or opt out of tracking. **BEST PRACTICE REC. 2** Update the website's cookie banner to include more specific information about web analytics data collection and provide direct links to relevant privacy information and user control options.

Dealing with personal information

2.4. Use or disclosure

APP 6 outlines the circumstances in which OAIC may use or disclose personal information that it holds.

Source	Summary of Principle	Analysis
APPs 6.1-6.3	The OAIC must not use or disclose personal information for a secondary purpose except if:	Based on the assessment above, the web analytics data collected is unlikely to constitute personal information. To

Source	Summary of Principle	Analysis
	• the individual the information is about has consented to the use or disclosure; • the secondary purpose is related to the primary purpose (or directly related in the case of sensitive information); or the circumstances in APPs 6.2 or 6.3 applies.	the extent APP 6 applies, the data is used solely for its primary purpose of website optimisation and performance analysis. No secondary uses or disclosures have been identified. No relevant findings.

2.5. Direct marketing

Source	Summary of Principle	Analysis
APP 7	Organisations must not use or disclose personal information for direct marketing purposes unless specific conditions are met. APP 7 may also apply to agencies in circumstances set out in section 7A of the Privacy Act.	APP 7 does not apply to the current web analytics implementation, and in any case the web analytics data is not used for direct marketing purposes No relevant findings.

2.6. Cross-border disclosure

APP 8 outlines the steps must take to protect personal information before it is disclosed overseas.

Source	Summary of Principle	Analysis
APP 8.1	If disclosing personal information to a recipient outside of Australia, the OAIC must: • take reasonable steps to ensure that any overseas recipients will not breach the APPs; or • reasonably believe that the recipient is subject to enforceable laws substantially like the APPs; or • inform an individual that overseas recipients may not apply the APPs to personal information about them, and the OAIC must obtain consent to the disclosure.	Based on the assessment above, the web analytics data collected is unlikely to constitute personal information. Google collects data directly from website visitors, stores it on servers primarily located in the United States, and processes the data under its own arrangements. In the interests of transparency, the OAIC's privacy policy appropriately informs users that data may be processed and stored overseas in connection with analytics services. The OAIC has configured GA4 with minimal data collection settings, limiting the scope of data collected by Google. No relevant findings.

3. Integrity of personal information

3.1. Quality

No relevant findings.

3.2. Security

APP 11 requires OAIC to take reasonable steps to protect personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure. OAIC must also destroy or de-identify personal information in certain circumstances.

Source	Summary of Principle	Analysis
APP 11.1	OAIC must take reasonable steps to protect personal information from misuse, interference, loss, unauthorised access, unauthorised modification and unauthorised disclosure.	Only authorised members of the OAIC web team will be able to access the GA4 platform, and this access will be limited to browser-based use with no external systems or third-party tools will be involved. Access to dashboards and analytics data will be granted only to staff who need it for their work, following a clear "need-to-know" principle. To maintain accountability and transparency, all user activity within GA4 will be logged in detail. These logs will help monitor how the platform is used and ensure that data is handled responsibly at all times.
APP 11.2	OAIC must take reasonable steps to destroy or de-identify personal information as soon as that information is no longer needed for the purposes of this activity (unless retention is required by law).	Data collected through GA4 will be stored on Google's servers for several years, in accordance with Google's data retention policies. The OAIC will not have direct control over permanently deleting this data once it is no longer needed. However, to help manage data visibility, GA4 is configured to automatically remove data from the reporting dashboard every two months. This means that while the data may still

Source	Summary of Principle	Analysis
		exist on Google's servers, it will no longer be accessible through the standard analytics interface after that period.

4. Access to, and correction of, personal information

4.1. Access

No relevant findings.

4.2. Correction

No relevant findings.

5. Data breach response

No relevant findings.

References and Key Terms

References to documents and key terms in this document are described below.

Term	Meaning
Australian Privacy Principles or **APPs**	means the 13 Australian Privacy Principles set out in Schedule 1 of the Privacy Act.
OAIC APP Guidelines	means the *Australian Privacy Principles guidelines* published by the Office of the Australian Information Commissioner at https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/.
OAIC PIA Guidance	means the *Guide to undertaking privacy impact assessments* published by the Office of the Australian Information Commissioner at https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-undertaking-privacy-impact-assessments/.
Personal Information	has the meaning given in the Privacy Act.
Privacy Act	means the *Privacy Act 1988* (Cth).
Sensitive Information	has the meaning given in the Privacy Act.

Attachment 1: GA4 dashboard reports

s47E(d)

s47E(d)

Search terms used within the websites search forms

	Search term	Page tile	Search term used
1.	(redacted)	Search	OAIC	45
2.	Credit report	Search	OAIC	39
3.	personal information	Search	OAIC	31
4.	AI	Search	OAIC	25
5.	optus	Search	OAIC	24
6.	sensitive information	Search	OAIC	23
7.	5303374830122935	Search	OAIC	20
8.	data breach	Search	OAIC	20
9.	consent	Search	OAIC	19
10.	incident	Search	OAIC	18
11.	annual report	Search	OAIC	17
12.	credit report	Search	OAIC	17
13.	privacy act	Search	OAIC	16
14.	Credit check	Search	OAIC	15
15.	Privacy Act 1988	Search	OAIC	15
16.	medibank	Search	OAIC	15
17.	privacy act 1988	Search	OAIC	15
18.	privacy policy	Search	OAIC	15
19.	privacy principles	Search	OAIC	15
20.	qantas	Search	OAIC	13
21.	privacy	Search	OAIC	13
22.	privacy impact assessment	Search	OAIC	13
23.	bunnings	Search	OAIC	13
24.	serious harm	Search	OAIC	12

Attachment 2: Information gathering interviews & materials

Interviews

	Date	OAIC attendees	elevenM attendees	Topics
1	30/6/2025	s47F s47F	s47F s47F s47F	Kick off meeting
2	04/7/2025	s47F	s47F s47F	Use of Web Analytics

Emails

	Date	Respondent	General topic
1	16/6/2025	s47F	Follow up questions on Web analytics

Documents

	Title
1	OAIC PIA – Google Analytics Privacy Impact Assessment
2	OAIC privacy policy accessed from https://www.oaic.gov.au/about-the-OAIC/our-corporate-information/plans-policies-and-procedures/privacy-policy on 18 July 2025.
3	Google Analytics Dashboard reports