IMAA

Data Governance and Privacy Principles

2026

IMAA Data Governance and Privacy Principles 2026

A Practical Framework for Independent Media Agencies
Prepared with the support of FMA Consulting

1. Why Data Governance and Privacy Matter Now

The media, advertising and digital ecosystem are undergoing major change driven by privacy regulation, reduced signal access, platform restrictions and rapid adoption of AI. Independent media agencies rely on trust, transparency and strong client relationships to compete in a market dominated by global holding groups and large technology platforms.

Strengthening privacy and data governance is now essential for protecting that trust, maintaining competitive advantage and ensuring long term success. The forewarned upcoming Privacy Act reforms will reshape expectations around transparency, consent, profiling, targeting and the handling of personal and inferred information. At the same time, major technology platforms are shifting toward more protected environments, increasing the importance of secure, ethical, unbiased and defensible data workflows.

Independent agencies excel because of their agility, creativity and local expertise. Embedding privacy first practices ensures these strengths remain a differentiator. It also helps agencies understand where they are today and where they may want to go next. Agencies do not need a formal maturity model, but having a general sense of whether current practices are informal, documented, consistently applied or optimised can help guide practical, risk based improvement over time.

Clear documentation and aligned agreements, including privacy policies, MSAs, terms of use and data processing terms, are also central to strong governance. They ensure the agency and client share a consistent understanding of how data is collected, used and protected.

The privacy and data landscape in Australia is also undergoing significant change. This document reflects both the current requirements of the Privacy Act and Australian Privacy Principles, and the Australian Government's proposed reforms arising from the Privacy Act Review. The proposed reforms are not yet law and may evolve throughout the legislative process. Where relevant, this document distinguishes between current obligations and anticipated changes to help agencies prepare responsibly and uplift their governance over time.

The IMAA will update this framework once the reforms are finalised so that members continue to have access to accurate, practical and up to date guidance.

2. Aim of This Document

This framework aims to:

- Provide clear, practical guidance for independent media agencies to manage data responsibly.
- Support agencies in preparing for Privacy Act reforms and evolving platform expectations.
- Strengthen trust with clients, consumers, partners and vendors.
- Embed privacy first practices across media, data, analytics and technology operations.
- Complement the existing IMAA AI Guiding Principles.
- Establish a shared language and baseline for privacy safe growth within the independent sector.

Agencies may adopt these principles flexibly, based on their maturity, structure and client needs.

Important

This framework is for general information and education only. It does not constitute legal advice and should not be relied on as legal advice. Agencies should seek independent legal or privacy advice on how the Privacy Act and Privacy Act reforms apply to their specific circumstances.

3. How to Use This Framework

Agencies can use this document to:

- Guide planning, buying, optimisation and reporting workflows.
- Support transparent client conversations on consent and data use.
- Improve pixel, tracking and measurement governance.
- Inform vendor due diligence and oversight.
- Strengthen documentation and audit readiness.
- Prepare for regulatory change.
- Upskill teams and increase privacy literacy.
- Promote trust and transparency across all client engagements.
- Ensure core documents, including privacy policies, MSAs, terms of use and data processing terms, are aligned with agreed data practices and expectations.
- Clarify data handling roles, including when the agency acts as a service provider or processor on behalf of a client.

This framework is scalable. Agencies can begin with the principles most relevant to their operations and expand over time.

4. The IMAA's Role in Supporting Members

The IMAA's mission is to support independent media agencies with:

- Education and capability building.
- Practical tools and shared templates.
- Access to trusted expert guidance.
- Advocacy in regulatory and industry discussions.
- Forums for collaboration, alignment and knowledge sharing.

4A. Understanding the Definition of Personal Information (Current vs Proposed)

The definition of personal information is already broad under the Privacy Act. The Australian Government's proposed reforms would expand and clarify this definition. These proposals are not yet law, and not all recommendations are expected to proceed in full.

Current law: what counts as personal information today

Under the Privacy Act and the Australian Privacy Principles, personal information is information or an opinion about an identified individual, or an individual who is reasonably identifiable. This includes:

- Names, email addresses, phone numbers and contact details.
- Account information and profile identifiers.
- Device identifiers where they reasonably identify a person.
- Online behaviour or activity linked to an identifiable individual.
- Location data linked to an identity.
- Any opinion, record or dataset tied to an identifiable individual.
- Inferred information where the inference is linked to an identifiable person. (Confirmed in OAIC targeted advertising and pixel tracking guidance.)
- Note : The term PII is not used under Australian law. Personal information is the correct definition.

Proposed changes: how personal information may expand

If adopted, the reforms would broaden and clarify the definition of personal information by adding non exhausted examples such as:

- Technical identifiers such as cookies, IP addresses and advertising IDs.
- Behavioural or engagement data used to profile or target an individual.
- Modelled, predicted or inferred information used to make decisions about an identifiable person.
- Persistent identifiers used to track a person across sites or services.
- Precise or granular location data, particularly where it identifies a person or reveals sensitive traits through patterns of behaviour.

These reflect the direction of reform but may not all proceed in full.

What this means for agencies

If these reforms are implemented, some datasets that agencies may previously have treated as non personal information may become regulated. This may affect:

- Targeting and optimisation.
- Cross site and cross device tracking.
- Lookalike, propensity and churn models.
- Identity and audience enrichment workflows.

Agencies should monitor reform progress and uplift governance, transparency and documentation so they can adapt when new laws are finalised.

4B. Understanding Sensitive Information (Current vs Proposed)

Sensitive information is a higher risk category under the current Privacy Act. The proposed reforms may expand how sensitivity is interpreted. These changes are proposals only and may be refined.

Current law: what counts as sensitive information today

Under the Privacy Act, sensitive information includes:

- Health information.
- Ethnicity, race or cultural background.
- Sexual orientation.
- Political opinions or memberships.
- Religious beliefs or affiliations.
- Biometric and genetic information.
- Criminal record.

Collecting sensitive information usually requires express consent unless a narrow exception applies.

Sensitive inferred information (current regulatory expectations)

While not part of the legal definition of sensitive information, OAIC guidance recognises that some inferences created through pixels, tags, analytics or optimisation may reveal sensitive traits. These include inferences about:

- Health status.
- Sexuality.
- Religious activity.
- Political views.
- Economic vulnerability or financial hardship.
- Other attributes that may expose an individual to discrimination or harm.

These are not legally classified as sensitive information, but the OAIC considers them high risk and expects stronger governance, justification, minimisation and transparency.
This aligns with OAIC pixel tracking and targeted advertising guidance.

Proposed changes: how sensitivity may be interpreted

The proposed reforms do not add new sensitive information categories, but they signal that:

- Inferences revealing sensitive traits may require stronger safeguards.
- Profiling or automated decisions using sensitive traits may require stronger justification or, in some cases, express consent under the proposed reforms.
- Precise or granular location data may be sensitive where it reveals patterns about health, religion, politics or financial hardship.

These changes are proposals only and may not all proceed.

What this means for agencies

Agencies may need to:

- Avoid or minimise processes that infer sensitive traits unless necessary, lawful and transparent.
- Apply stronger governance to vendors, pixels and third party tools that generate or access sensitive inferences.
- Treat economic vulnerability, financial hardship or other sensitive inferences as high-risk, even though they are not sensitive information under the law.
- Document decisions about whether to include or exclude sensitive attributes or sensitive inferences in modelling, targeting or optimisation workflows.

4C. What Consent Looks Like (Current vs Proposed)

Consent already plays an important role under the Privacy Act. The proposed reforms aim to clarify and strengthen the standard. These changes are still proposals and may evolve during drafting.

Current law: consent under the Australian Privacy Principles

Consent must be:

- Voluntary
- Informed
- Current and specific
- Given by someone with capacity

Consent is currently required for:

- The collection of sensitive information unless an exception applies.
- Use or disclosure of personal information for a purpose that is not reasonably expected.
- Certain high-risk activities identified in OAIC guidance, such as some forms of cross-site tracking or profiling.

Cross border disclosure under APP 8 does not generally require consent. Organisations must take reasonable steps to ensure overseas recipients comply with the APPs or rely on another

accountability mechanism. Under APP 5, individuals must be notified if their personal information will be disclosed overseas and the countries involved.

Common misconception: Consent is not generally required for cross-border disclosure under APP 8. However, agencies remain accountable for how personal information is handled overseas and must ensure appropriate safeguards and transparency are in place.

Proposed changes: a clearer and higher standard

If adopted, consent would need to be:

- Voluntary and free of pressure or manipulative design.
- Informed, using clear and plain language.
- Specific for each purpose.
- Unambiguous.
- Easy to withdraw and respected across systems.

Situations where consent may be required under proposed reforms

Proposed reforms suggest higher expectations for:

- High-risk targeted advertising and profiling.
- Cross site tracking and third party pixel activity.
- Collection or use of precise or granular location data.
- Use of inferred or modelled data linked to an identifiable person.
- Use of children's data in high risk contexts.
- Automated decision making with significant effects.

What this means for agencies

Agencies should uplift:

- Consent flows and wording.
- Evidence of consent capture and management.
- How consent signals are passed through adtech and data supply chains.
- Oversight of consent management platforms.
- Documentation and governance for sensitive information and sensitive inferences.

Agencies that prepare early will be well placed once reforms are finalised.

5. IMAA Data Governance and Privacy Principles (2025)

Each principle includes:

- Why it matters.
- What to avoid.
- What to prioritise.

These principles align with OAIC guidance, the Australian Privacy Principles, Privacy Act reform proposals, ISO/IEC 27701, ISO/IEC 42001, the NIST Privacy Framework and leading global privacy practices.

Before applying the principles, agencies should review Sections 4A, 4B and 4C which explain current and proposed definitions of personal information, sensitive information and consent. This context will help agencies interpret the principles correctly and plan a measured uplift path.

Principle 1: Privacy by Design Across All Workflows

Why this matters

Privacy by design is a core expectation of OAIC guidance and upcoming reforms. Embedding privacy early reduces risk, avoids rework and builds trust across all stages of media planning, activation and reporting.

Avoid

- Late stage privacy checks.
- Collecting unnecessary identifiers.
- Deploying tracking without review.

Prioritise

- Early privacy consideration in planning.
- Consent aware workflows.
- Documented decision making.
- Vendors with transparent data practices.

Principle 2: Legal, Fair and Consent Based Data Use

Why this matters

Consent, fairness and lawful use are central to the APPs and underpin the majority of upcoming Privacy Act changes.

Avoid

- Repurposing data beyond its original purpose.
- Using datasets without clear consent.
- Relying on legacy consent models that are no longer defensible.

Prioritise

- Clear lawful purpose.
- Verified consent that aligns with Section 4C.
- Reviewing data source and origin.
- Ensuring data use is fair and consistent with reasonable expectations.

For a more detailed overview of current and proposed consent requirements, agencies should refer to Section 4C.

Principle 3: Data Minimisation and Purpose Limitation

Why this matters

Minimisation reduces risk and supports compliance with APP 3 and reform expectations. Agencies should only collect and use information that is necessary and clearly tied to purpose.

Avoid

- Excessive tracking.
- Broad or undefined data capture.
- Retaining data without a clear purpose.

Prioritise

- Limiting events to what is needed.
- Clear use cases.
- Regular deletion cycles.

Principle 4: Preparing for Privacy Act Reforms

Why this matters

Privacy Act reforms introduce broader definitions of personal information, new expectations around fairness, tighter consent requirements, rules on targeting and profiling, and stronger consumer rights. Agencies must prepare early to remain compliant and competitive.

Avoid

- Outdated privacy practices.
- Reliance on sensitive inferred attributes.
- Legacy targeting models that ignore reform impacts.

Prioritise

- Reviewing disclosures and documentation.
- Assessing profiling, targeting and optimisation workflows.
- Planning for uplift in consent, transparency and governance.
- Monitoring updates from government, OAIC and industry bodies.

For context on how personal information, sensitive information and consent may change, agencies should review Sections 4A, 4B and 4C.

Principle 5: Ethical Audience Use and Targeting Standards

Why this matters

Ethical targeting protects consumers, maintains trust and supports compliance with reform expectations around fairness and profiling.

Avoid

- Sensitive inferred audiences, especially where they suggest health, financial stress, sexuality, children's vulnerabilities or other protected traits, which may require express consent under proposed reforms.
- Optimisation signals that exploit vulnerabilities.
- Unreviewed or opaque modelling.
- Targeting or profiling involving children's data without strong justification, safeguards and transparency.

Prioritise

- Ethical audience definitions that exclude or strictly govern sensitive categories.
- Reviewing optimisation inputs and models for potential bias or harm.
- Targeting aligned to consent and purpose.
- Clear client discussions about audience risks and safeguards.

Principle 6: Pixel Governance and Tracking Oversight

Why this matters

OAIC pixel guidance highlights significant risks related to data leakage, piggybacking vendors and consent failure.

Avoid

- Unapproved pixels.
- Hidden third party piggybacking.
- Tags firing without consent.
- Pixels that capture precise location or sensitive inferences without express consent.

Prioritise

- Verified tag inventory.
- Consent aware triggering and sequencing.
- Periodic tracking audits.
- Reviewing pixels and tags for collection of granular or precise location data or sensitive categories.

Principle 7: Transparency in the Digital Supply Chain

Why this matters

Clients expect clarity around vendor relationships, data movement and platform touchpoints.

Avoid

- Unknown downstream vendors.
- Unclear data flows.
- Reliance on opaque optimisation.

Prioritise

- Mapping data flows end to end.
- Understanding vendor data usage.
- Transparent client communication.

Principle 8: Vendor Accountability and Due Diligence

Why this matters

Vendors influence how data is collected, processed and shared. Strong oversight reduces privacy, operational and reputational risk.

Avoid

- Vendors who repurpose or resell data.
- Offshore processing without disclosure.
- Weak contractual protections.

Prioritise

- Vendor privacy and security reviews.
- Strong data processing terms.
- Reviewing vendor access and governance.

Principle 9: Security of Client and Consumer Data

Why this matters

APP 11 requires organisations to take reasonable steps to protect personal information. Security forms the foundation for all other privacy protections.

Avoid

- Weak access controls.
- Shared or unmanaged credentials.
- Unsecured transfers or storage.

Prioritise

- Access management and role based controls.
- Encryption in transit and at rest.
- Secure storage and transmission practices.

Principle 10: Data Accuracy and Responsible Use

Why this matters

Under APP 10, agencies must ensure data is accurate, complete and up to date. Good data quality improves decision making and reduces risk of harm or misinterpretation.

Avoid

- Stale or unreliable datasets.
- Combining datasets that may enable re identification.
- Unsupported or misleading assumptions.

Prioritise

- Applying oversight and review to automated or AI-assisted decisions that may materially affect individuals.
- Reviewing data provenance.
- Regular refresh cycles.
- Documented assumptions and interpretations.

Principle 11: Client Collaboration and Data Transparency

Why this matters

Agencies and clients share responsibility for privacy outcomes. Alignment across documentation, expectations and data practices reduces risk and strengthens trust.

Avoid

- Activating unverified client data.
- Adding tracking without agreement.
- Using data beyond the agreed purpose.

Prioritise

- Joint reviews of data use, tracking and vendor access.
- Documentation aligned with client expectations.
- Consent and purpose validation.
- Ensuring privacy policies, MSAs and terms of use reflect agreed practices.
- Clear data processing and role definitions.
- Clear definition of data ownership, where the client owns its first party data and the agency acts as a service provider or processor unless otherwise agreed in writing.

Principle 12: Documentation and Audit Readiness

Why this matters

Clear documentation supports accountability, defensibility and operational trust. It ensures agencies can demonstrate how decisions were made and what data processes were approved.

Avoid

- No central record of approvals.
- Untracked vendors or subprocessors.
- Missing or outdated tag inventories.

Prioritise

- Vendor summaries and access records.
- Tag and pixel inventories with clear ownership.
- Decision logs for key data and tracking choices.

6. Recommended Resources

- Office of the Australian Information Commissioner (OAIC)
  APPs, pixel guidance, data breach guidance.
  https://www.oaic.gov.au

- Australian Government Privacy Act Reforms
  Reform process and updates.
  https://www.ag.gov.au/rights-and-protections/privacy

- Australian Cyber Security Centre (ACSC)
  Security best practice including the Essential Eight.
  https://www.cyber.gov.au

- Digital Transformation Agency (DTA)
  Australian Digital Service Standards and governance guidance.
  https://www.digital.gov.au/standards

- International Association of Privacy Professionals (IAPP)
  Global privacy governance resources, training and certifications.
  https://iapp.org

- NIST Privacy Framework
  Privacy risk management framework.
  https://www.nist.gov/privacy-framework

- NIST AI Risk Management Framework
  Responsible AI governance and risk guidance.
  https://www.nist.gov/itl/ai-risk-management-framework

- ISO/IEC 27701
  Privacy Information Management System standard.
  https://www.iso.org/standard/27701

- ISO/IEC 42001
  AI management and governance standard.
  https://www.iso.org/standard/81230.html

7. Glossary of Key Terms

Artificial Intelligence (AI)
Systems or models capable of performing tasks that normally require human intelligence, including prediction, classification, analysis, optimisation, generation or automated decision making.

Anonymisation
The irreversible removal of personal identifiers so that an individual cannot be re identified in any context. True anonymisation is difficult to achieve in digital advertising.

Attribution
The process of assigning credit for a conversion or outcome to one or more media touchpoints using tracking signals, tags, identifiers or modelled assumptions.

Behavioural Data
Data derived from user actions such as browsing, clicking or viewing. Under the proposed reforms, behavioural data may be considered personal information if it identifies an individual or profiles them.

Consent
A voluntary, informed, specific and unambiguous agreement for the collection or use of personal information. Under the proposed reforms, consent must also be easy to withdraw and consistently respected across all systems and vendors. See Section 4C.

Cross Site Tracking
Collection of signals, identifiers or behavioural data across multiple websites or apps to understand journeys, measure attribution or support targeting.

Data Leakage
The unintended transmission of data from a site, pixel, tag or vendor to a party that should not receive it. Often caused by piggybacking tags, unclear vendor chains or misconfigured pixels.

Data Minimisation
Limiting the collection of personal information to what is reasonably necessary for the intended purpose.

De identification
Removing or modifying identifiers so individuals are not reasonably identifiable. Unlike anonymisation, de identified data can often be re identified through linkage with other datasets.

Device Identifier (Device ID)
A unique ID linked to a mobile or connected device, such as IDFA or GAID. Under the proposed reforms, device identifiers are treated as personal information.

First Party Data
Information collected directly from interactions with an advertiser's owned channels, such as sites, apps, CRM, call centre or offline interactions.

Granular Location Data
Location data with sufficient resolution to understand a person's movement patterns or visits to potentially sensitive locations. Under the proposed reforms, granular or precise location data may be treated as sensitive information where it reveals sensitive traits.

High Risk Processing / High Impact Processing
Activities that involve significant privacy or ethical risk, such as profiling, targeted advertising using sensitive traits, granular location tracking, automated decision making or cross site tracking.

Identifier (Technical Identifier)
A piece of technical data used to distinguish a device or user, including cookies, IP addresses, device IDs, MAIDs, login IDs and hashed emails. Proposed reforms confirm these are personal information when linked to an individual.

Identity Data
Any set of identifiers or attributes used to recognise or authenticate an individual across systems. Includes email addresses, phone numbers, login details, hashed identifiers and persistent IDs.

Inference or Inferred Data
Information derived from analysis, prediction or modelling of other data points. Examples include interest predictions, purchase intent scores or churn likelihood. Proposed reforms may classify inferred data as personal information.

Lookalike Modelling
Using machine learning to identify people similar to a known audience or customer group. May involve inferred or modelled personal information.

Modelled Data
Statistical predictions or generated values about an individual or group, such as propensity scores, value segments or intent predictions. May be treated as personal information under the proposed reforms.

Personal Information (PI)
Information or an opinion about an identified or reasonably identifiable individual. Under the proposed reforms, PI would explicitly include technical identifiers, behavioural data, persistent IDs and inferred or modelled information. See Section 4A.

Persistent Identifier
Identifiers used to track or recognise an individual across multiple domains or systems. Examples include device IDs, login IDs, hashed emails, RampID and ID5.

Pixel / Tracking Pixel
A small piece of code used to measure user actions, track journeys or send data to a platform. Pixels must be governed carefully to avoid data leakage or unintended collection.

Piggybacking
When a pixel or tag loads additional third party scripts without the knowledge or approval of the publisher or agency, potentially causing data leakage.

Profiling
Automated processing of personal information to analyse or predict behaviour, interests or preferences. Profiling may receive additional regulatory controls under the proposed reforms.

Purpose Limitation
The principle that personal information should only be used for the purpose it was collected for, or a directly related purpose the individual would reasonably expect.

Reasonably Identifiable
An individual is reasonably identifiable if they can be identified from the data alone or in combination with other information likely to be available.

Sensitive Information
A higher risk category of personal information that includes health, ethnicity, sexuality, political opinions, religious beliefs, biometrics, genetic information and criminal history.Under the proposed reforms, the concept of sensitive information may expand to include sensitive inferences and granular or precise location data where it reveals sensitive traits. See Section 4B.

Sensitive Inference
A sensitive attribute or trait that is inferred through modelling, analysis or optimisation rather than directly collected, such as inferred sexuality, health conditions or financial stress.

Supply Chain Transparency
Documented visibility over all vendors, subprocessors and platforms that access, process or receive client or consumer data. Essential for consent, fairness and defensibility.

Tag Management System (TMS)
Software used to manage, control and deploy pixels and tracking tags. Examples include Google Tag Manager and Tealium. TMS governance is central to pixel oversight.

Targeting
Selecting audiences or users based on characteristics, behaviours, interests or predicted outcomes. Targeting must align with consent, fairness and purpose.

Third Party Data
Information collected by an organisation that does not have a direct relationship with the individual. Higher governance, consent clarity and due diligence are required.

Vendor
Any external provider that accesses, processes or receives data within agency workflows, including ad servers, DSPs, SSPs, analytics platforms, identity partners and measurement tools.

8. Looking Ahead

Privacy expectations, platform requirements and regulatory settings will continue to evolve. These principles are intended as a living framework that the IMAA will review periodically to ensure alignment with member needs and best practice.

About FMA Consulting

https://fmaconsulting.net/

FMA Consulting is an independent Australian advisory practice that helps independent media agencies adopt AI and data driven technologies in safe, practical and commercially effective ways. We specialise in privacy first growth, AI governance and modernising media and data operations. Our work supports agencies with clear frameworks, practical tools and hands on guidance tailored to their size, capability and clients.

Our services

- Privacy and compliance advisory including preparation for Privacy Act reforms, pixel and tracking governance, consent and data handling guidance, and privacy by design support.
- AI strategy and governance including safe AI use cases, AI policies and lightweight governance frameworks.
- Media technology and AdTech consulting including platform audits, supply chain transparency, vendor assessment, workflow optimisation and programmatic safety.
- Operational tools and templates including checklists, risk frameworks, consent flows, privacy review tools, AI assessment templates and implementation guides.
- Capability building and training for planners, strategists, client service teams and leadership, with real use cases and practical scenarios.

Contact Details : info@fmaconsulting.net

Website https://fmaconsulting.net

About the IMAA

The Independent Media Agencies of Australia is the national industry body representing Australia's independent media agencies. The IMAA promotes the benefits of working with independent agencies, supports collaboration and capability development and champions one hundred percent Australian owned businesses.

Disclaimer

This document provides general guidance and does not constitute legal advice. Agencies should seek independent legal or privacy advice where required.