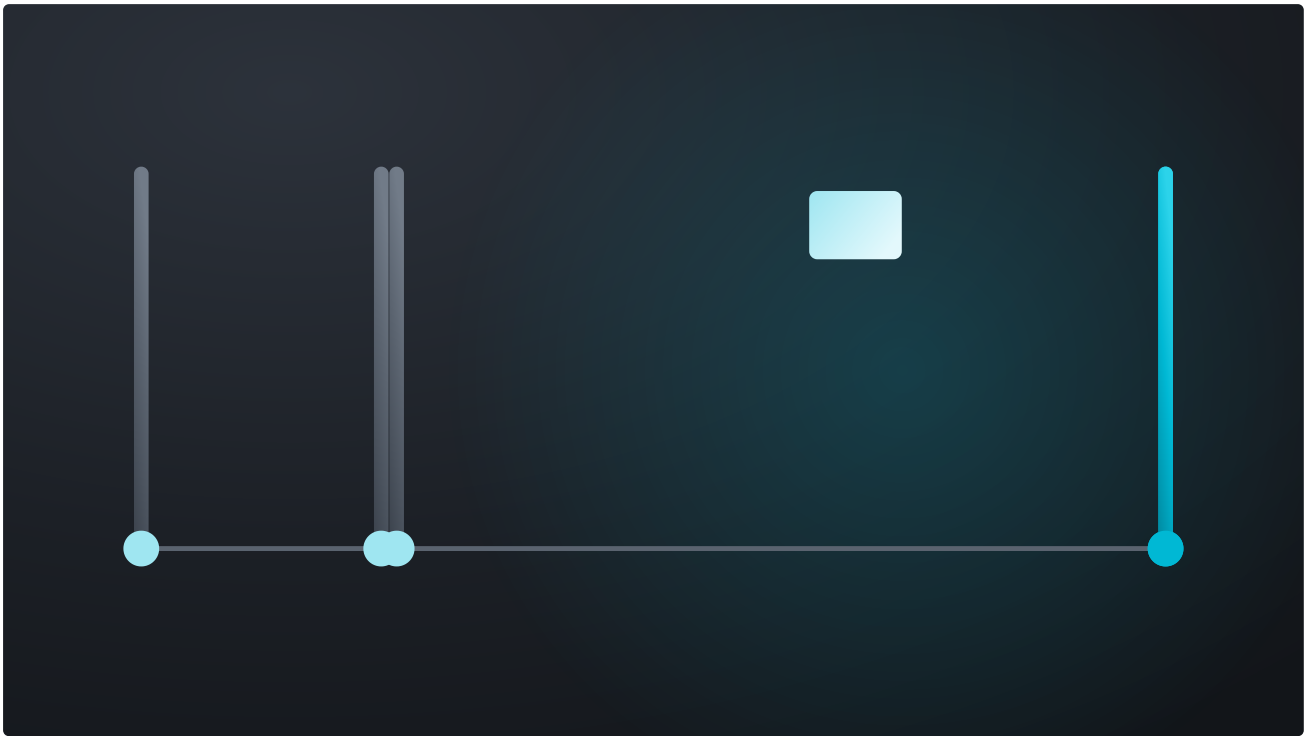
Black Shard

RESEARCH REPORT

The Privacy Act reforms, dated: what has commenced and what starts on 10 December 2026

Most of the first round of privacy reform is already law. The two obligations left on the calendar land together on 10 December 2026, and both are answered by reading what your software does with personal information and writing it down.



Entity	Black Shard Pty Ltd · ABN 66 696 910 773
Document ID	BS-RPT-12
Classification	Public
Version	1.1
First published	11 August 2026
This edition	29 October 2026
Figures	Dates checked 11 Aug 2026

Executive summary

The Privacy and Other Legislation Amendment Act 2024 received Royal Assent on 10 December 2024, and most of its privacy reforms commenced the next day, 11 December 2024. Since 11 December 2024 the reasonable steps APP 11 requires an entity to take to protect the personal information it holds expressly include technical and organisational measures, and the clarification applies to information held after that day whether or not it was collected before it.

The statutory tort for serious invasions of privacy commenced on 10 June 2025, six months after Royal Assent, and gives an individual a cause of action in court against any person who seriously and intentionally or recklessly invades their privacy. Mandatory ransomware payment reporting under the Cyber Security Act 2024 commenced on 30 May 2025 for businesses with an annual turnover of $3 million or more and for entities responsible for critical infrastructure.

On 10 December 2026 the automated decision-making transparency requirements in APP 1.7 to 1.9 commence, and the Children's Online Privacy Code must be registered by the same day. From 10 December 2026 an APP entity that has arranged for a computer program to use personal information to make a decision that could reasonably be expected to significantly affect an individual's rights or interests, or to do a thing substantially and directly related to making it, must say so in its privacy policy, whether the arrangement was made before or after that day.

For a firm that holds customer data the calendar is now short. The reforms already in force changed what a court and the regulator can do after a breach or a misuse; the two that commence in December change what a privacy policy has to say before one. Both December obligations are met by the same piece of work: a list of every place personal information flows through your systems, and a statement of which of those flows a program decides on its own.

A team that runs that review before November has its December wording ready, and the wording describes the system as it runs. A team that writes the policy in December describes the product it remembers building.

- List every flow of personal information through your systems, including the suppliers, models and analytics services that receive it.
- Name each decision a program makes or shapes about a person, and whether a person reviews it.
- Rewrite the privacy policy from that list before 10 December 2026, and set a date to read it against the system again.

Method

Every date comes from the commencement table of the Act as the Federal Register of Legislation publishes it, read beside the register's making date, or from the page on which the Office of the Australian Information Commissioner states it. Every date is printed as the source states it; each source was on the register or the OAIC's pages by 11 August 2026 and is listed at the end.

The commencement table fixes most dates by a formula, the day after Royal Assent or a period of months beginning on it, and the register fills in the calendar date. The two formulas that matter are the twenty-four months that set 10 December 2026 and the six months that set 10 June 2025. The tort could have commenced earlier by proclamation; it commenced on the fallback day the formula names.

The ransomware reporting date belongs to a different Act and is printed from the Australian Signals Directorate's annual threat report, because a firm planning its privacy calendar plans that one beside it.

The review a software team runs before December

The review has three passes. The first pass is the data map: every field of personal information the product collects, every table and bucket it rests in, every supplier, model and analytics service it is sent to, and the purpose that was written down when the field was added. Fields with no written purpose are the first finding.

The second pass is the decision list. Walk every place where code, a rule or a model decides or shapes something about a person: an eligibility check, a fraud score that holds an order, an identity match that fails closed, a ranking that decides who is shown a service, an automated refusal. For each one, write what personal information feeds it, whether the output is the decision or an input to a person, and what the person affected is told. That list is the raw material of the December wording.

The third pass is the policy itself. Read the current privacy policy against the two lists and mark every sentence the system no longer bears out. Then add the automated decision wording, the kinds of information those programs use and the kinds of decisions they make or shape, in plain words a customer can act on. The policy is published before 10 December 2026 and the two lists are kept with it, because the question a regulator asks after a complaint is what the entity knew about its own processing.

If the product is likely to be reached by children, the same review feeds the Code work: whether the service is a social media, relevant electronic or designated internet service, what it collects from a child and why, and what it would take to turn each collection off.

What has commenced

The Privacy and Other Legislation Amendment Act 2024 received Royal Assent on 10 December 2024, and most of its privacy reforms commenced the next day, 11 December 2024. Since 11 December 2024 the reasonable steps APP 11 requires an entity to take to protect the personal information it holds expressly include technical and organisational measures, and the clarification applies to information held after that day whether or not it was collected before it.

THE REFORM DATES, DECEMBER 2024 TO DECEMBER 2026

Two obligations land on 10 December 2026; the statutory tort and ransomware payment reporting are already in force. Source: Federal Register of Legislation commencement table for the Act, OAIC pages and the ASD annual threat report, checked 11 August 2026.

The security clarification matters more than its length suggests. The reasonable steps duty has always been read with technical measures in mind; the amendment writes them into the principle, so a firm whose breach came through an unpatched service or a shared password now argues against the text of the principle when it calls its steps reasonable. It applies to information held today, whatever the date it was collected.

The statutory tort

The statutory tort for serious invasions of privacy commenced on 10 June 2025, six months after Royal Assent, and gives an individual a cause of action in court against any person who seriously and intentionally or recklessly invades their privacy. The elements are an intrusion into seclusion or a misuse of information, a reasonable expectation of privacy, intent or recklessness, seriousness, and a public interest in privacy that outweighs any countervailing public interest. The invasion is actionable without proof of damage.

For a small firm the tort is the change that reaches below the Privacy Act's turnover line. The Schedule that creates it is read separately from the rest of the Act and the defendant is any person. The exemptions it names are narrow: intelligence agencies and law enforcement bodies, people who disclose information to them or use information they disclose, people under eighteen, and journalists in their work. A business that reads a customer's messages or publishes their details can be sued whatever its turnover.

Ransomware payment reporting

Mandatory ransomware payment reporting under the Cyber Security Act 2024 commenced on 30 May 2025 for businesses with an annual turnover of $3 million or more and for entities responsible for critical infrastructure. A firm under the line has no duty to report a payment. A firm above it that pays, or has a payment made on its behalf, now has one, so the decision to pay is also a decision to report, and the facts of the payment are written down on the day.

What starts on 10 December 2026

On 10 December 2026 the automated decision-making transparency requirements in APP 1.7 to 1.9 commence, and the Children's Online Privacy Code must be registered by the same day.

Automated decisions in the privacy policy

From 10 December 2026 an APP entity that has arranged for a computer program to use personal information to make a decision that could reasonably be expected to significantly affect an individual's rights or interests, or to do a thing substantially and directly related to making it, must say so in its privacy policy, whether the arrangement was made before or after that day. The privacy policy must then state the kinds of personal information those programs use, the kinds of decisions made solely by them, and the kinds of decisions in which they do a thing substantially and directly related to the decision.

The test is wide. A decision includes a refusal or a failure to decide; doing a thing includes refusing or failing to do it; and the rights or interests affected may be helped as much as harmed. The Act's own examples are a decision to grant or refuse a benefit under a law, a decision that affects a person's rights under a contract or arrangement, and a decision that affects access to a significant service or support. A lender's eligibility rule, a marketplace's seller suspension and a clinic's booking triage all sit inside that.

The obligation is transparency and the duty falls on the policy. Nothing in the amendment stops a program deciding; it requires the entity to have found out which of its programs do, and to say so. It applies to decisions made after it commences even where the program, the data and the arrangement were in place before it, so a product shipped in the year before December is inside it from the first day.

The Children's Online Privacy Code

The Commissioner must develop and register the Children's Online Privacy Code within 24 months of Royal Assent, which sets the registration deadline at 10 December 2026. The OAIC consulted on the draft Children's Online Privacy Code from 31 March 2026 to 5 June 2026. The Code will bind a provider of a social media service, relevant electronic service or designated internet service that is likely to be accessed by children and is not providing a health service, and any other APP entity the Code specifies.

The Code is an APP code: it sets out how one or more of the principles apply to the privacy of children, and it binds the entities it names in the way it names them. A business that provides a health service is outside the first limb even where children use it, and the Commissioner may add classes of entity and may exclude them. The final text is the OAIC's to register; what a software team can settle before it lands is whether its service is likely to be accessed by children and what it collects from them.

The Commissioner must publish a draft and take submissions for at least sixty days before registering it, and that consultation ran from the end of March to the start of June. The next move is the OAIC's, and the registration date is fixed in the Act whatever the OAIC does.

What to do

For a firm with customer data, the order to follow before December:

1. Build the data map: every field of personal information, where it rests, every supplier, model and analytics service it reaches, and the written purpose for each.

2. List every decision a program makes or shapes about a person, with the information that feeds it, whether a person reviews it, and what the person affected is told.
3. Rewrite the privacy policy from the two lists, with the automated decision wording in plain words, and publish it before 10 December 2026.
4. Decide whether your service is likely to be accessed by children, and if it is, write down what it collects from them and how each collection is switched off.
5. Read the reasonable steps duty against your estate: patching on a clock, phishing-resistant sign-in on every account that reaches personal information, and backups a compromised administrator cannot delete.
6. Hold less: delete fields with no written purpose and shorten retention where the purpose has ended, because the tort and the breach scheme both reach information you still hold.
7. If your turnover is above the reporting line, write the ransomware decision procedure now: who decides, who reports, and what is written down on the day.
8. Put a date in the calendar to read the policy against the system again, and keep the two lists with it.

We run this review for clients: the data map and the decision list drawn from the running system and its code, the privacy policy rewritten from them with the December wording, and the reasonable steps read back from the systems that enforce them, with a dated list of what remains. For software teams we do the privacy policy work inside the build, so the policy ships with the release that changes it. Scope and price are at blackshard.com.au/services/compliance.

Our record

Black Shard builds and defends the systems Australian organisations run on. We keep the data map and the decision list for our own platforms, and we hold the records that let a buyer check it.

The record is as held at 29 October 2026, the date this edition was revised.

- SMB1001:2026 Gold, issued by CyberCert, valid 16 Jun 2026 to 17 Jun 2027.
- Essential Eight Maturity Level 3, assessed September 2026.
- Prequalified supplier to Queensland councils under Local Buy arrangement LB308, ICT Solutions, Products, Services and New Technologies.
- Prequalified supplier under the NSW Government ICT Services Scheme (SCM0020).
- Holder of Victorian Fair Jobs Code pre-assessment certificate FJC-261023-11119, required for Victorian Government threshold and high-value procurement.
- Our CISO holds the Exemplar Global ISO/IEC 27001:2022 Lead Auditor credential.
- Professional indemnity, public liability, cyber and workers' compensation insurance, all current.
- More than 65,000 tests across our repositories, counted on 26 October 2026.
- More than 1,500 deploys and releases shipped since 1 January 2026.

> 24/7 incident line: 1800 370 270.

Sources

- Federal Register of Legislation, Privacy and Other Legislation Amendment Act 2024, made 10 December 2024, registered 13 December 2024: https://www.legislation.gov.au/C2024A00128/latest/text
- OAIC, Statutory tort for serious invasions of privacy, 19 June 2025: https://www.oaic.gov.au/privacy/your-privacy-rights/more-privacy-rights/statutory-tort-for-serious-invasions-of-privacy
- OAIC, Children's Online Privacy Code, 19 March 2026, updated 5 August 2026: https://www.oaic.gov.au/privacy/privacy-registers/privacy-codes/childrens-online-privacy-code
- OAIC, Children's Online Privacy Code public consultation report, 20 November 2025: https://www.oaic.gov.au/privacy/privacy-registers/privacy-codes/childrens-online-privacy-code-public-consultation-report
- Australian Signals Directorate, Annual Cyber Threat Report 2024-2025, 14 October 2025: https://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/annual-cyber-threat-report-2024-2025
- Privacy Act 1988 (Cth), the Australian Privacy Principles