Privacy Act 2025: Employee Awareness & Training

Suttons

What is the Privacy Act?

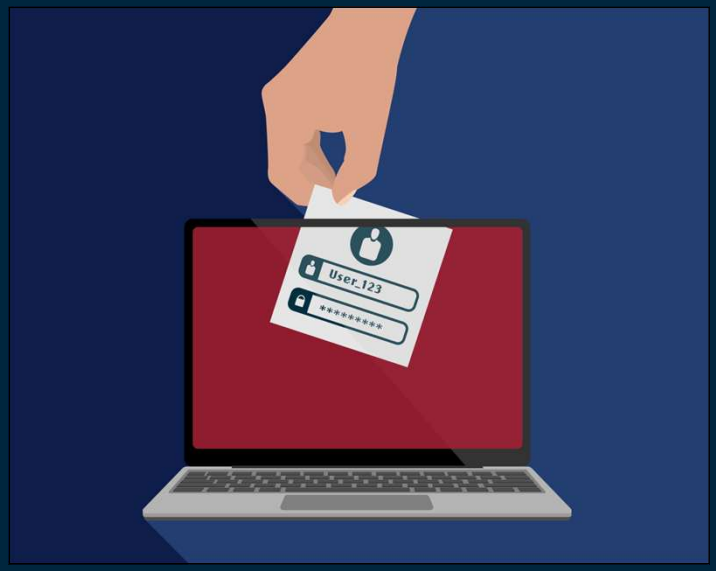
The Privacy Act 1988 defines personal information as any data that identifies or could identify an individual (in any format) and sets rules for how organisations must handle this data.

The Privacy Act 1988 was outdated because it didn't address modern data practices.

Aspect	Pre-1988	Now / 2025
Data Storage	Paper files stored in offices	Digital storage on cloud, devices, apps
Data Sharing	Minimal, mostly in-person or mail	Frequent sharing via apps, social media, email, third-party platforms/ websites
Access & Interaction	Physical access only, limited staff handling	Instant digital access, multiple employees and systems can view and use data
Accountability	Business responsible	Both employees and businesses can be personally liable for breaches

Key Drivers of Change

- Data breaches have increased across Australia, creating a need for stronger protections.
- The public has demanded better safeguards for personal information.
- The law now allows individuals to sue for serious invasions of privacy, even when no financial loss has occurred.
- Emotional distress caused by a privacy breach can now be grounds for legal action.



Suttons

Why the Privacy Act Changed?

- Between 2019 and 2021, the number of data breaches in Australia increased significantly, **exposing millions of customer records**.
- In 2022, high-profile breaches at **Optus and Medibank** exposed sensitive identification and medical data, sparking national concern.
- By 2023 – 2024, public trust in data security had declined, with **75% of Australians fearing their data was not safe**.

Suttons

What Has Changed?

Inclusion of New **“Serious Invasion of Privacy”** Statutory Tort in Australia for Privacy is Now in Effect

June 2025 – Privacy Act 1988 Updated

- Now includes **Statutory Tort** for Serious Invasions of Privacy
- Privacy Act introduced a Statutory Tort, allowing individuals to take legal action for serious invasions of privacy.

“Stronger protections, greater accountability, and restored trust in how personal data is handled”

Suttons

Statutory Tort for Serious Invasions of Privacy

What is a Statutory Tort?

"A Statutory Tort is legislation that creates the right to sue for specific harms, with defined liability standards and remedies."

- The new Statutory Tort allows individuals to take legal action for Serious Invasions of Privacy.
- Employees can be sued personally if their actions breach someone's privacy.
- Emotional distress is sufficient to bring a legal claim against you personally.

Suttons

Before vs After

Before	After
Only businesses could be fined	Individuals can now be sued personally
Must prove financial loss	Emotional distress sufficient
Limited staff accountability *(could be fined, but not sued)*	Increased personal responsibility for everyone

Overlap & Synergy of the Privacy Act and Serious Invasion of Privacy Statutory Tort

Under Australia's updated privacy laws, a single data breach can now result in both government fines under the Privacy Act and personal lawsuits from affected individuals under the new Statutory Tort.

Example: A company's employee leaks customer data. The OAIC (Office of the Australian Information Commissioner) may penalise the company under the Privacy Act, while affected customers could sue the *employee* personally under the Statutory Tort.

What Counts as a “Serious Invasion of Privacy”

A **Serious Invasion of Privacy** occurs when:

Intentional/ Reckless Intrusion	There is a deliberate or reckless violation of privacy (e.g., unauthorised surveillance, hacking, or physical trespass).
Highly Offensive	The intrusion would be deemed highly offensive to a reasonable person.
Reasonable Expectation of Privacy	The individual had a legitimate expectation of privacy in the context (e.g., private property, personal communications).
No Public Interest Justification	If sharing someone’s private info causes real harm and isn’t clearly helping the public.

Why This Matters to Suttons

- We handle highly sensitive customer data every day, including names, dates of birth, driver's licenses, credit card details, and voice recordings.
- Our customers trust us to keep their information safe.
- A single mistake can result in legal action against **you and the business**, mandatory public reporting, fines, lawsuits, and reputational damage.
- **The updated Privacy Act (including Statutory Tort) now holds you personally accountable for serious breaches**.

Suttons

Real World Examples

- A former Business Manager / Sales Consultant retaining customer data and using it after leaving the company.
- A Manager accessing an employee's medical records without consent.
- Customer IDs stored on an unsecured personal phone.
- Service RO's and sales contracts left in plain sight of other customers.
- Customer details / data being left in pre-owned inventory (i.e., logbooks, old contracts of sale, previous service history, etc.)
- Sharing customer service invoices or sales contracts with non-authorised recipients.

Common Risks in Dealerships

- Improper disposal of records or payment details creates risk.
- Accessing records without a valid work-related reason is a violation.
- Leaving contracts or other documents on desks or printers can expose customer information.
- Sending customer IDs via unsecured emails is unsafe.
- Accessing customer data on a personal phone without using Suttons authorised systems (i.e. Outlook, Dealer Socket App) with your Suttons login and credentials.
- Employees may store customer data on personal devices, which is unsafe.

Suttons

No Customer Data Stored on Personal Phones

- Personal phones lack Suttons-authorised security protocols, encryption, and controlled access.
- They are vulnerable to theft, hacking, and malware, putting customer data at immediate risk.
- Storing customer data on personal devices violates Suttons' Privacy Policy and puts you at risk.
- This practice bypasses mandated data storage, encryption, and secure disposal methods required by law.
- Use only **Suttons approved** systems for all customer data storage and communication, e.g., Dealer Socket and Dealer Drive.

Suttons

Authorised Company Platforms

Customer data **must not** be stored on personal devices.

All Company data must be accessed and saved exclusively through **Suttons-authorised** platforms using company-issued login credentials. Approved platforms include (but are not limited to):

- Microsoft Outlook
- Business CRM applications (e.g. DealerSocket, Drive Expert)

Suttons

Additional Risks

- Sharing customer data without proper consent or safeguards is a serious risk (i.e., password-protected).
- Leaving documents in view where others can see them should be avoided.
- Releasing documents without confirming the recipient's identity is unsafe.

<u>If you identify a risk, escalate it to your manager immediately.</u>

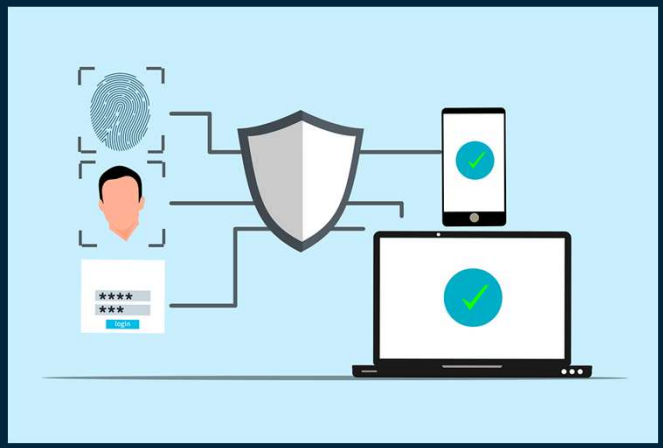
Suttons

Legal and Practical Responsibilities

Do's	Don'ts
Always and ONLY use customer data only for the purpose it was collected	Don't store customer data on personal devices or personal email accounts
Collect only the information that is necessary	Don't store data "just in case"
Store and access data only in secure, Suttons authorised systems	Don't access records unless our role requires it
Dispose of outdated information following company protocols	Don't leave customer information unattended
Report any breaches or potential breaches immediately (to the Financial Controller)	Don't share data without verifying consent and following security protocols

How to Protect Yourself & the Business

- Use multi-factor authentication and **Suttons-authorised systems**.
- Verify the **recipient's identity** before sharing any documents.
- Always keep **customer data secure**.
- **Dispose securely** of outdated information.
- If you notice a risk, **escalate it to your manager** immediately.
- **Only use customer data for the specific purpose for which it was collected**.



Maximum Penalties for Corporations

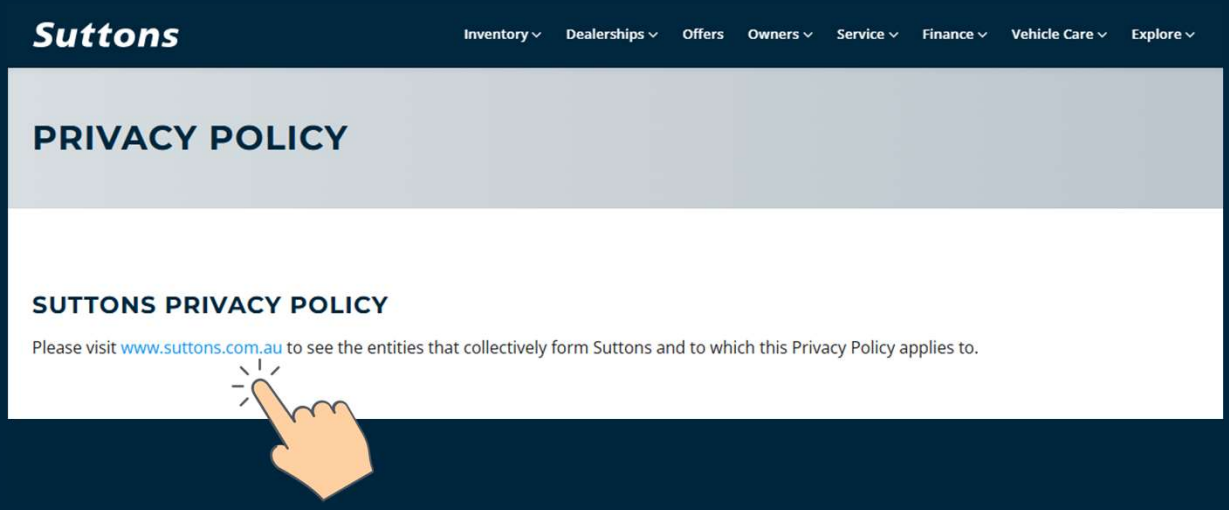
Whichever is Higher
$50 million *or*
Three times the benefit of the breach (if calculable) *or*
30% of the body corporate's adjusted turnover during the breach period (if the benefit cannot be determined)

Privacy Breach Penalty Tiers for Individuals

Tier	Applies to	Penalty
Tier 1	Infringement Notice, specified privacy breaches	**$66,000** per breach
Tier 2	Serious Interference with privacy attracts a higher penalty than a standard infringement notice	Up to **$660,000** per breach
Tier 3	Court-determined based on: • The information sensitivity • The number of people affected & the impact on them • If the breach was repeated or ongoing • **Failure to implement adequate privacy practices**	Up to **$2.5 million** per breach

Where to Get Help

- Your first point of contact is the dealership Financial Controller and General Manager who will escalate to Suttons Privacy Officer (John Vanderjagt).
- Should you have any questions about sharing customer information, please contact Customer Care by calling 02 8711 8619 or emailing customercare@suttons.com.au
- The Suttons Privacy Policy is available at: Suttons Privacy Policy



Incident Reporting Process

- If you identify a risk, escalate it to your manager immediately.

If a breach occurs

- Notify your Financial Controller and General Manager immediately.

- Remember a single mistake can cost you and the business and have serious implications for the customer. Stay vigilant.

Suttons

Closing Reminder

One mistake can cost you and the business.

Protect our customers.

Protect yourself.

Protect Suttons.

Suttons