Compliance Checklist for Businesses

Under the Updated Australian Privacy Act (2023–2025 Reforms)

Introduction

The Australian Privacy Act 1988 is undergoing significant reforms to strengthen privacy protections, bring Australia closer to international standards (like the GDPR), and respond to increasing cyber risks. This guide provides a practical checklist to help businesses, large or small, prepare for and comply with the updated obligations.

🔑 1. Understand Your Data & Obligations

☐ Map all personal information collected, used, stored, and shared, including IP addresses, cookies, and other identifiers.
☐ Verify whether your business is exempt (e.g., < AUD 3M turnover).
☐ Identify if you process employee records, these may soon be covered by the Act.
☐ Review and update contracts with third parties to ensure privacy compliance.

📝 2. Privacy Policy & Notices

☐ Update your privacy policy to reflect broader definition of personal information and rights to access, correction, erasure, and objection.
☐ Make privacy notices clear, concise, and accessible.
☐ Disclose use of cookies, tracking, and analytics transparently.

💼 3. Governance & Accountability

☐ Designate a Privacy Officer or responsible contact.
☐ Integrate privacy by design and by default into projects and processes.
☐ Conduct regular Privacy Impact Assessments (PIAs) for high-risk activities.
☐ Implement a data minimization policy.

🔐 4. Security & Breach Readiness

☐ Strengthen data security measures.
☐ Update your Data Breach Response Plan to meet the notification requirements.
☐ Train staff on breach reporting procedures.
☐ Conduct breach simulation exercises.

🧹 5. Individual Rights Management

☐ Set up processes to respond promptly to access and correction requests.
☐ Handle erasure (“right to be forgotten”) requests.
☐ Enable individuals to object to uses like direct marketing.
☐ Document all requests and responses.

📊 6. Regulatory Engagement & Monitoring

☐ Stay updated on OAIC guidance and legislative changes.
☐ Be prepared for audits and keep clear compliance records.
☐ Cooperate with the OAIC if directed and implement any orders promptly.

👥 7. Staff Awareness & Training

☐ Train all employees on privacy principles and updated requirements.
☐ Provide specialised training for staff handling personal data and breaches.

📌 Optional Best Practices

☐ Consider privacy certifications or seals of compliance.
☐ Align with GDPR standards for international consistency.
☐ Participate in public consultations on reforms.
