Brighter

Personally Identifiable Information (PII) Website Security Checklist

To ensure the security and privacy of Personally Identifiable Information (PII) collected through your website, follow the actionable items below. For a more detailed explanation, please refer to our comprehensive article at insights.brighter.com.au/pii-security

Inform and Obtain Consent from Users

- □ Clearly inform users about data collection and its purpose
- □ Obtain explicit consent before collecting PII

Secure Data Storage

- □ Ensure form field data is encrypted when stored
- □ Implement access controls for authorised personnel only
- □ Keep your website system up to date (ie. Brighter Maintenance Plan)

Data Retention

- □ Enforce data retention settings on your web forms
- □ Make sure you have a process in place for easy data deletion by user-request

Email Notifications

- □ Avoid including sensitive PII in emails
- □ Use encryption methods like TLS for email security
- □ Train staff on secure email handling and phishing recognition

External System Integrations

- □ Secure API connections with strong authentication (e.g., OAuth)
- □ Conduct regular audits of PII within third-party service providers

General Security Practices:

- □ Use MFA (multi-factor authentication) for your website CMS
- □ Schedule regular website security assessments and vulnerability scans
- □ Establish an incident response plan for data breaches
- □ Provide staff training on data protection and security practices