Privacy and mobile apps: a checklist for app developers

☑ Your privacy responsibilities

Your agency or organisation (which may just be you) is responsible for all personal information collected, used and disclosed by your mobile app.

- ☑ Identify someone to be responsible for privacy protection.
- ☑ Use a Privacy Impact Assessment[1] to map where the information is going, identify potential privacy risks, and assist with privacy planning (including 'privacy by design').[2]
- ☑ Put in place controls, such as conditions of contract or user agreements, to ensure that third parties accessing personal information through your app respect their privacy obligations.

☑ Be open and transparent about your privacy practices

- ☑ Develop a privacy policy that clearly and simply informs users what your app is doing with their personal information.
- ☑ Make your app's privacy policy easy for users and potential users to find.
- ☑ Put in place a monitoring process to ensure that personal information is being handled in the way described in your privacy policy.
- ☑ When updating an app, inform users of any changes to the way their personal information is handled, and seek express consent to any changes that could impact on their privacy.

☑ Obtain meaningful consent despite the small screen challenge

- ☑ Select the right strategy to convey privacy rules in a way that is meaningful on the small screen. This could include:
  - 'short form notices', with important points up front and links to more detailed explanations

[1] See www.oaic.gov.au/privacy/privacy-resources/privacy-guides/privacy-impact-assessment-guide
[2] www.privacybydesign.ca/index.php/about-pbd/

- a privacy dashboard that displays a user's privacy settings and provides a convenient means of changing them
- cues such as graphics, colour and sound to draw user attention to what is happening with their personal information, the reasons for it, and choices available to the user.

☑ Timing of user notice and consent is critical

- ☑ Obtain consent at the point of download.
- ☑ Tell users how their personal information is being handled at the time they download the app and in-context when they use the app to ensure that their consent is meaningful and relevant.
- ☑ Consider how best to deliver privacy messages to most effectively capture users' attention and achieve the most impact at the right time, without causing notice fatigue.

☑ Only collect personal information that your app needs to function

- ☑ Limit data collection to what is needed to carry out legitimate purposes.
- ☑ Do not collect data just because you think it may be useful in the future.
- ☑ Allow users to opt out of the collection of their personal information, or if that is not practicable, clearly explain they cannot opt out so they can make an informed decision whether to use the app.
- ☑ Delete or de-identify personal information that you no longer need for a lawful purpose.

☑ Secure what you collect

- ☑ Put in place appropriate safeguards to protect the personal information you are handling. Use encryption when storing and transmitting data.
- ☑ Give users the ability to delete or request the deletion of all of the data that your app has collected about them.
- ☑ Publish clear policies about how long it will take to delete personal information once a user stops using your app.
- ☑ Delete personal information that you no longer need for a lawful purpose.

Find out more about privacy and apps, including resources for using icons to represent privacy information, in the OAIC's *Mobile privacy: a better practice guide for mobile app developers*.