Mobile and Privacy

Accountability Framework for the implementation of the GSMA Privacy Design Guidelines for Mobile App Development

Introduction

The GSM Association and its members have been working on a mobile privacy initiative (MPI) and reaching out to the broader mobile ecosystem since 2009 to address consumer privacy concerns and foster confidence and trust for mobile users. In addition to establishing a set of Mobile Privacy Principles, a key outcome of this work is the GSMA Privacy Design Guidelines for Mobile App Development ('the Guidelines')[1], published in February 2012.

A number of GSMA members have already begun to implement these Guidelines across their own-branded apps and have created a framework by which implementing organisations can demonstrate their accountability. The principle of 'accountability' is gaining importance and is included in privacy and data protection laws and standards around the world[2]. It was first established in the OECD Guidelines[3] in 1980. In data protection terms, 'accountability' is generally regarded as the commitment to, and acceptance of, responsibility for protecting personal information in compliance with laws or other standards. Accountability also refers to the ability of an organisation to demonstrate its compliance with such laws and related promises – "say what you do, and do what you say."

Objective of the accountability framework

1. To help organisations demonstrate that their business practices comply with the Guidelines.
2. To be applicable across different international regions of operation.
3. To help foster the confidence and trust of customers and other stakeholders.

Accountability framework – core components

To ensure a robust and comprehensive accountability framework, which generates confidence and trust in the effectiveness of the Guidelines, a range of organisational and technical measures should be incorporated, including:

- procedures and practices
- oversight and redress
- remediation of noncompliances[4].

The five elements of accountability outlined by the Center for Information Policy and Leadership (CIPL)[5] are considered as a good starting point to build a robust accountability framework. These five elements are common in other proposals and business practices and include:

1. Organisational commitment to accountability and adoption of internal policies (consistent with the Guidelines).
2. Mechanisms to put privacy policies into effect, including tools, training and education.
3. Systems for internal, ongoing oversight and assurance reviews (and external facing verification).
4. Transparency and mechanisms for individual participation.
5. Means for remediation and enforcement.

[1] www.gsma.com/newsroom/gsma-announces-new-initiative-addressing-mobile-app-privacy/

[2] The Asia Pacific Economic Cooperation (APEC) Privacy Framework, the Madrid Resolution, the proposed EU General Data Protection Regulation, the Canadian Personal Information Protection and Electronic Documents Act

[3] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data http://www.oecd.org/sti/interneteconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

[4] The Online Behavioural Advertising industry's self-regulatory program of privacy principles were highly criticised when first launched for lacking clearly defined and robust policies and practices for ensuring compliance in practice. www.loeb.com/onlineadvertisingcomplianceoba/ see Also the Article 29 WP Opinion 16/2011 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp188_en.pdf

[5] www.huntonfiles.com/files/webupload/CIPL_Galway_Accountability_Paper.pdf and CIPL www.informationpolicycentre.com/accountability-based_privacy_governance/

Key elements of the accountability framework

The accountability framework builds on the CIPL five elements and incorporates the components outlined below. Implementation examples have been included to aid understanding.

1. Organisational Commitment:

Implementing organisations **will:**

- **Obtain senior management buy-in and sign off.** This is considered essential to ensuring organisations commit to adopting the Guidelines and appropriately resource their implementation.
- **Appoint a responsible person who will:**
  - help establish program controls
  - liaise and coordinate with internal teams
  - help establish reporting structures and remediation mechanisms for addressing noncompliances.

2.Internal program controls (mechanisms) for giving effect to the Guidelines:

Implementing organisations **will:**

- **Establish a policy requiring the organisation to implement the Guidelines.**

  *The policy **should** reflect management commitment and agreed reporting structures and responsibilities, and **may** include references to other applicable policies and procedures.*

- **Incorporate the Guidelines into the development and review process.**

  *This **may** include a personal information checklist to identify what information an app is accessing, collecting, sharing and using, and for what purposes. A checklist **may** help identify specific privacy risks and how these can be addressed.*

- **Establish mechanisms for customers to report complaints and incidents and ensure those reports are captured to address concerns and improve the Guidelines.**

  *Organisations **should** establish the means to capture reports and enquiries to aid investigation and remediation, and the continuing effectiveness of the framework and the Guidelines.*

  *Organisations **may** create focus groups to test the impact of the Guidelines on customer experience and feedback into development process and broader Mobile Privacy Initiative.*

- **Establish contractual and other organisational arrangements with third parties** who develop apps under the commissioning organisation's brand name or who collect and independently use personal information about users of those apps with the commissioning organisation's explicit knowledge.

- **Establish a program to educate** relevant parties on the importance of privacy and their roles and responsibilities under the framework and the Guidelines.

  *Organisations **should** educate developers (internal and external), customer service agents and other employees on the importance of app privacy, the requirements of the Guidelines and any relevant policies, processes and procedures they are required to follow.*

- **Establish a system of ongoing oversight, assessment and remediation**, to ensure the effectiveness of the framework is measured and any weaknesses and failings are addressed in a timely and effective manner.

  *Organisations **should** establish program controls to ensure that the applicable Guidelines have been effectively incorporated in the apps review process. These program controls **may** form part of a company's existing Privacy Impact Assessment and Information Security Management System methodology.*

  *Organisations **may** systematically or randomly test apps for compliance. Testing may be based on a percentage of total apps. More frequent testing **may** be applied to apps that hold greater privacy risks to individuals.*

  *Organisations **should** establish mechanisms by which employees may report noncompliances, issues or concerns and by which these may be addressed.*

- **Establish external reporting to self-certify incorporation of the Guidelines.**

  *Current processes and mechanisms for measuring and reporting on corporate social responsibility objectives **may** provide a vehicle for reporting on compliance with the framework and by which companies may self-certify and report on their implementation of the Guidelines.*

- **Establish internal enforcement policy and mechanisms for noncompliances.**

  Organisations should document what action they will take against third party developers who fail to comply with the Guidelines either (a) when developing apps under the commissioning organisation's brand name or (b) when using the commissioning organisation's brand name under contract.

The above core components are considered to be the minimum necessary components to ensure the Guidelines are successfully implemented.

3. Enforcement for noncompliant organisations

The GSMA's MPI is considering a range of tools and methodologies to help identify noncompliances[6]. Where an organisation is found to be noncompliant with the Guidelines, the MPI **will** take action proportionate to the identified noncompliance. Such action **may** include:

- For minor noncompliance, the MPI **will** initiate a discussion with the participating organisation to identify and agree areas for remediation. Remediation plans agreed with the MPI **will** be implemented in a timely fashion.
- Continued noncompliances or serious breaches **will** be referred to the appropriate governing subcommittee of the GSMA Board – the GSMA Public Policy Committee – to identify and implement an appropriate sanction, up to and including public expulsion from the programme for repeated noncompliances.

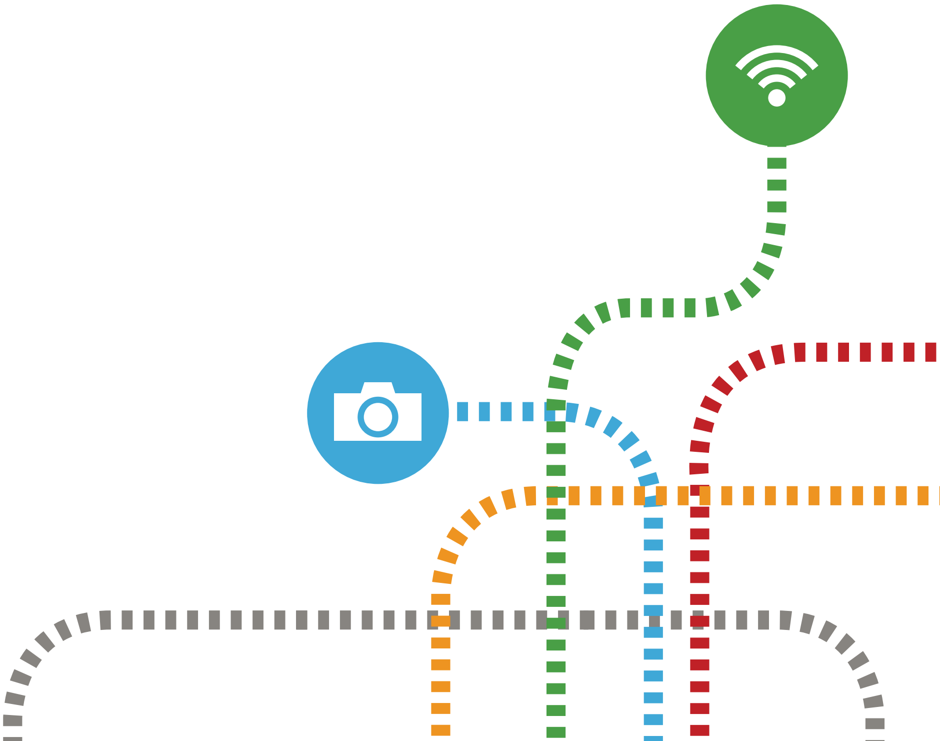
For more information contact:

Natasha Jackson
Head of Content Policy, GSMA
njackson@gsma.com

Pat Walshe
Director of Privacy, GSMA
pwalshe@gsma.com

www.gsma.com/mobileprivacy

[6] For example, external app transparency tools and testing mechanisms to which a random sample of participating apps may be submitted.



GSMA Head Office
Level 7, 5 New Street Square
New Fetter Lane
London EC4A 3BF
United Kingdom

Tel: +44 (0)207 356 0600
Email: mobileprivacy@gsma.com

www.gsma.com/mobileprivacy