Mobile and Privacy

Privacy Design Guidelines for Mobile Application Development

February 2012

Table of contents

Introduction

Background

The emergence of open mobile platforms and the convergence of mobile and the 'web' has created a vibrant and dynamic mobile ecosystem that enables individuals to shape and present rich personal identities online, connect with communities of their choice, and engage with innovative, applications and services. Much of this relies on the real-time access and use of personal information that is often transferred globally between applications, devices, and companies.

While these abilities serve as a powerful enabler for innovative business models and the personalisation of applications and services, they may also provide a vehicle for malicious or surreptitious access to a user's personal information. Even applications that legitimately access and use personal information may fail to meet the *privacy expectation of users and undermine their confidence and trust in organisations and the wider mobile ecosystem*. Problems occur when users are not given clear and transparent notice of an application's access to and use of their personal information, or when they are not given an opportunity to express meaningful choice and control over the use of their information for secondary purposes and beyond that necessary to the operation of an application or service.

The GSMA recently published a set of universal mobile privacy principles that describe the way in which mobile consumers' privacy could be respected and protected. These guidelines seek to articulate those principles in functional terms for mobile application design.

Scope

These guidelines apply privacy design principles to applications and their related services designed for mobile devices. They are intended to apply to all parties in the application or service delivery chain that are responsible for collecting and processing a user's personal information – developers, device manufacturers, platforms, and OS companies, mobile operators, advertisers and analytics companies.

Purpose

Applications and their related services should create good privacy experiences and engender trust and confidence. Key to realising these objectives is a robust and effective framework for the protection of privacy, based on the principles of transparency, choice and control.

These guidelines adopt a *Privacy by Design* approach and are intended to help ensure that mobile applications are developed in ways that respect and protect the privacy of users and their personal information. *Privacy by Design* is also about recognising that users have privacy interests (expectations, needs, wants and concerns) that must be addressed in a proactive manner from the start and not as an afterthought or an 'add-on'. The guidelines encourage the development, delivery and operation of mobile applications that put users first and help them understand (at a minimum):

- what personal information a mobile application may access, collect and use
- what the information will be used for, and why, and
- how users may exercise choice and control over this use.

Examples are provided with each guideline and some illustrative use cases are presented in a separate Annex.

Definitions

Active consent: This means a user is given a clear opportunity to agree a specific and notified use of their personal information. Active consent would apply to secondary non-obvious use of a user's personal information, and/or applications that have additional privacy implications for users such as an app requesting a user's location where such data is not necessary to the functioning of the application. Active consent must be captured in a way so that consent is not the default option.

Application: Where we use the term 'Application' or 'App', we intend it to be broad in scope; it may include a native application, an application or script running within a specific runtime, or a widget or script running within a browser environment.

Location data: Information that identifies the geographical location of a user's device, which may include Cell ID, GPS, Wifi or other less granular information such as village or town.

Personal information: There are lots of legal definitions of personal information, but in its simplest terms, it means information that relates to an individual and that you could use to identify them, contact or locate them.

Personal information may include:

- data collected directly from a user via an application's user interface (name, address, date of birth)
- data that is gathered indirectly such as mobile phone number, IMEI or UDID
- data gathered about a user's behaviour, such as location data, web-browsing data or the applications used which is linked to a unique profile
- user-generated data such as contact lists, videos and photos, messages, emails, notes, and call logs.

To be identified, an individual need not be known by name – a user may be identified even when their information is associated only with a unique identifier such as a Unique Device Identifier.

There are categories of information that may be considered '**sensitive**' and which may need additional security. This may, for example, include log-on credentials, registration and financial details, and information about a person's health for example.

Privacy: Privacy is a dynamic concept that can mean different things to different people. For the purposes of these guidelines, privacy is defined as the ability of individuals to know how their personal information will be collected, shared and used, and to exercise choice and control over its use.

User: The end user of applications and related services.

Transparency, choice and control — putting the user first

A key aspect of fostering confidence and trust in applications is being open with users and letting them know:

- who's collecting and using their personal information
- why personal information is being used
- what personal information is being shared, with whom and for what purposes.

Users should have enough information to make an informed choice about whether to use an application and the consequences of doing so. Some of this information may be obvious before a user downloads or activates an application and so makes no additional disclosures about an application necessary.

In short:

- **Be transparent:** Tell users who you are, what personal information you require, what you intend to do with it and who you intend to share it with (and why!) — but don't overburden them with prompts!
- **Help users manage their privacy**: Make them aware of an application's privacy default settings.
- **Give users easy to understand choices and mechanisms for managing their privacy:** Make it easy not hard — they'll like you better for it.

Guideline	Implementation	Use case and examples
TCC1 **Do not surreptitiously access or collect personal information.** An application must not secretly access and collect personal information about users.	Before a user downloads or activates an application, he or she must be presented with information about: • what personal information an application will access, collect and use • what personal information will be stored (on the device and remotely) • what personal information will be shared, with whom it will be shared • and for what purpose	An application must not access a user's location if the application isn't a location based service app. If location data is secondary to the app and needed to meet other commercial objectives then you need to get a user's active consent (see the 'location privacy' section below). An application must not access and use contact details held in a device's address book unless this is part of the apps functionality clearly explained to

Guideline	Implementation	Use case and examples
Users must be made aware about the collection and use of their personal information upfront, enabling them to make informed decisions about using an application or service.	• how long personal information will be kept • any terms and conditions of use affecting a user's privacy. Prompt the user and make this information easy to discover and understand. Keep it simple and make it easy to exercise choice. Enable the user to reject the installation or activation if they do not wish their personal information to be used as explained to them. Ensure usability and avoid excessive user prompts that will burden the user. Consider the user experience.	users. Transparency is key. Tell users what information you need and why you need it — then keep to your word. If you change your mind at a later stage and want to use personal information for another purpose that's different from what you originally told users, then you'll need to go back to them and tell them about any new uses and get their agreement.
TCC2 **Identify yourself to users** Users must know who is collecting or using their personal information and how they can contact that entity for more information or to exercise their rights.	Before a user downloads or activates an application, he or she must be made aware of the identity of any entities that will collect or use personal information in the scope of the application, including a company or individual name and a country of origin. Users must have easy access (via a link or menu item) to brief contact details of the organisation.	The app landing page is an excellent place to publish key privacy facts, contact information and provide a hyperlink to a more detailed privacy statement. There is no single solution to providing users with information about you, your organisation, their privacy and what you'll do with their data. Be creative and encourage users to explore how best to manage their privacy — but don't burden them and keep it simple and easy.

Guideline	Implementation	Use case and examples
TCC3 **Let users exercise their rights.** Provide users with enough information so they can reasonably be expected to know how to access and correct any personal information you might hold about them.	Provide a short and genuinely informative privacy statement explaining in clear simple terms how people can get a copy of their personal information or correct and update information supplied by them or held by you.	As above, the app landing page may provide an effective place to give users simple clear notice or direct them to more detailed information about how to exercise any privacy rights.
TCC4 **Minimise information you collect and limit its use.** Information collected by an application should be reasonable, not excessive, and used within the scope of the user's expectations and other legitimate business purposes as notified to users.	Think about what personal information you need and then justify it. Is it really necessary? Are you required to collect it, share it or keep it to meet a business need or legal obligation? An application must access, collect and use only the minimum information required: • to provision, operate or maintain the application • to meet identified business purposes that you've told the user about or to meet legal obligations. Use personal information in ways users would expect when they made a decision to download or activate an application.	If you require access to contact list data, identify which fields are necessary to fill a particular feature of the application and collect no more than the specific field(s) required. Do not use that data for additional non-obvious purposes unless the user has agreed to this.
TCC5 **Where necessary, gain the user's active consent** Sometimes users will need to give	In the majority of cases, it will be obvious to users what personal information will be needed to support an application. However, where access, collection and use of personal	Applications that do not use location for any of the features or functionality of an application requested by a user may not collect location for other purposes — for example, targeted advertising or analytics —

Guideline	Implementation	Use case and examples
their active consent to the use of their personal information. a) Collection or use of personal information not necessary to the application's primary purpose,	information is not necessary to an application's primary purpose and would be unexpected by the user, then users should be given a choice about whether to allow these secondary and non-obvious uses of their information. Other situations may also require active consent: Social networks and social media, Mobile advertising, Location, Children and adolescents (as detailed in the sections below). Where it is necessary to get active consent, users should be made aware of: • how long a consent is valid • how they can manage any consent given by them • the consequences of withholding or withdrawing their consent. Users must be able to withdraw consent by simple and efficient means, without any undue delay or undue cost.	unless the user gives their active consent.
b) Sharing personal information with third parties.	If third parties will collect or have access to user information for their own purposes, the user must be made aware at the earliest opportunity that their data will be shared, indicating:	Applications should not include third-party code that collects and analyses personal information to target users with advertising, without the active consent of the user.

Guideline	Implementation	Use case and examples
	• with whom it will be shared and for what purposes, and • providing links to those third parties' and their privacy notices. Users must be allowed to choose whether to allow this collection, access and use by third parties.	
c) Storing personal information after immediate use of the application.	If user data will be retained after the immediate use of an application, users must be given information about: • the periods for which information may be retained and why • how the user can exercise specific rights over their information.	
TCC6 **Give users control over repeated prompting.** Where possible, users should have choices about how – and how often – they are reminded about features and functionality that use their personal information.	Where technically possible, provide users with opportunities to determine how they will be prompted and how often they will be prompted to make decisions over access to, and use of, their personal information. Privacy by Design means putting the user first and helping them become aware of and manage the privacy implications of apps and	Users may be given the choice to 'remember' their log-on credentials, billing address, email addresses, or location. It is possible to provide blanket one-time prompting for each data type or granular more context-specific prompts. For example, users may be given the choice of allowing an application to access device location permanently, for a specified period or to select to be

Guideline	Implementation	Use case and examples
	services, in ways that enhance the user's privacy experience.	prompted periodically by email, text, in-app notice or icon.
TCC7 **No silent ('secret') updates.** Users must agree to any changes to an application that affect their privacy.	Users must be told about a material change to the way an application will collect or use their personal information, before such a change is implemented, so that they can make an informed choice about whether to continue to use the application. Consent to changes can be obtained in two ways: 1. For changes that are essential to an application's continued operation: Notice that a change will occur and a chance to disable the application. 2. For changes that the user may choose to adopt: A prompt with choices about whether to allow the change or continue with the previous functionality.	This does not prevent remote 'over the air' type updates that are necessary to maintain the primary functionality and integrity of an application or service. The guideline **would apply**, for example, where an app suddenly wished to access and upload contact details stored on a user's device or device location data.

Data retention and security

Security can exist without privacy, but there can be no privacy without security. Make sure that you are adequately protecting the personal information a user has entrusted you with, on the handset and wherever you store or transmit personal information.

Think about why you need to retain a user's personal information and how long you need to keep it. Can you justify it? Personal information that is retained indefinitely decreases in value over time, but it increases in cost and risk. Identify how long a piece of personal information remains necessary to your business model (as opposed to desirable), and make sure to securely delete it when it's no longer required. Setting retention periods for your data (as short as necessary) makes good business sense, can help to manage risk and costs, and to avoid regulatory action or bad publicity if things go wrong (because you kept it for too long and the data's been compromised).

Guideline	Implementation	Use case and examples
DRS1 **Actively manage identifiers.** Where an application creates or uses a unique identifier, take measures to ensure the identifier is linked to the rightful application user and keep this information up to date.	Each party that uses identifiers is responsible for taking measures to: • ensure any unique identifiers apply to only one unique user • ensure unique identifiers are kept up to date and kept only for as long as necessary to fulfill the applications purpose and reasons notified to users • prevent a unique identifier being associated with another user unless required by a justified business need (see *Use case and examples*).	Mobile operators may reassign identifiers such as MSISDN (mobile numbers) to other customers without the application being aware of it. If you capture a user's MSISDN you should take measures to ensure this information is accurate and up to date by periodically confirming with the user. Likewise, device manufacturers may assign unique device IDs (UDID). Mobile users may replace their mobile phones and sell them on to other individuals. Unless care is taken, the new owner of the mobile could easily be associated with the Unique Device Identifier or other unique identifier associated with the previous owner. That association and linking could have consequences for the online privacy experiences

Guideline	Implementation	Use case and examples
		of the new owner and his or her use of the device. Each party that collects and uses UDIDs is responsible for ensuring they meet this guideline.
DRS2 **Keep data secure.** Take appropriate steps to protect users' personal information from unauthorised disclosure or access.	Adopt technical measures and business processes to prevent the misuse or corruption of personal information. Where an application creates or collects personal information considered **sensitive**, such as log-on details, UDIDs, mobile numbers, contact details, financial details, such information must be stored and transmitted in a secure manner.	Collecting and keeping certain types of information when it's simply not necessary creates the risk that it can be lost, stolen, and misused. If you need to collect, transmit and retain sensitive information such as a user's financial payment details or log-on details, then you should secure this data by using encryption or a suitable hashing mechanism and delete it when it is no longer needed.
DRS3 **Authenticate where security calls for it.** Authenticate users where possible using risk-appropriate authentication methods.	Where the assertion of a real-world identity is an important component of a service, stronger authentication should be implemented, such as two-factor authentication using a mobile handset and UICC. Consider using CAPTCHAs and RE-CAPTACHAs to help differentiate bona fide members from spammers. Use technical tools to restrict spidering and bulk downloads or access without network permission.	
DRS4 **Set retention and deletion periods.**	Justify the collection and retention of personal information according to identified business	Data stored in a behavioural profile relating to a unique user by a cookie or other device identifier,

Guideline	Implementation	Use case and examples
Personal information that is to be retained must be subject to retention and deletion periods that are justified according to clearly identified business needs or legal obligations.	needs or legal obligations. Set a policy and implement it at a technical and business process level. Once personal information is no longer required to meet a specific legitimate business purpose or legal requirements/obligations, it should be destroyed or anonymised. Truly anonymous data may be retained indefinitely. To anonymise data, remove any information that could be used to identify a specific individual, ensuring it is not possible to re-identify the individual, and ensure that the data cannot be related to a single, unidentified individual by unique identifiers.	even with no other identifiable information, would not be considered truly anonymous. A profile with the unique identifier removed or hashed may be considered anonymous.

Education

It is important that users can understand how best to manage their privacy and protect their personal information, by providing them with clear and simple information about privacy options and security settings of applications. It's about helping users to be aware of privacy and security issues and how to manage them.

Guideline	Implementation	Use case and examples
E1 **Educate users about the privacy implications and settings of your app or service and how they can manage their privacy.**	Provide users with information about the privacy and security settings and capabilities of applications and services and how to activate and manage these to help them protect and control their own privacy. This information should be clearly signposted using simple, non-technical language. Users should be provided with details of how to protect their privacy in general, by directing them to online resources and sites.	Users could be directed to a developers or app store's own privacy and security pages, or other initiatives such as: - www.getsafeonline.org - www.onguardonline.gov/topics/mobile-apps.aspx - www.staysafeonline.org/in-the-home/mobile-devices-0 which provide tips on Smartphone and app privacy and security.

Social networking and social media

Socially enabled applications allow users to connect to and share information with a community of other users or the general public. These kinds of applications may hold significant privacy implications and should include privacy-protective default settings and clear information and instructions so that users know how the choices they make affect their privacy.

It is important to ensure users can make genuinely informed decisions about engaging in social networking services and can exercise appropriate privacy choices.

Guideline	Implementation	Use case and examples
SNS1 **Prompt users to register for social networks, but be careful about mapping registration information to public profiles.**	Require users to register and create an account before using the service and clearly indicate to the user when information is voluntary. Do not automatically map user registration information to the user's publicly available profile unless the user has been made aware of this and given the option to exercise choice and control. See below.	If the privacy default setting for a social network account is 'public' then users should be made aware of this before supplying any personal information and setting up an account, and they must be given the opportunity to agree or decline.
SNS2 **Ensure default settings are privacy protective and give users control of their personal profiles in ways that are easy to understand and use.**	Users should be made aware in a very transparent and clear manner, about the privacy setting of their profile and how data about them may be shared with or made available to others. Users should know: • what information or categories of information will be published about them upon registering • how they can easily change any default settings	It is a good idea to provide a privacy education page to help users understand how they can manage their privacy. This could include advice that information they make 'public' will be searchable by online search engines.

Guideline	Implementation	Use case and examples
	- whether they and their personal information will be searchable by or alerted to other users - how they can make data 'private' visible only to authorised parties. It must be intuitively clear to users what information in their profile is public, what information is published to a limited group (such as friends) and what information is completely private (only visible to the user). Users must have the ability to review all of their profile data, including user-generated, usage and derived data.	
SNS3 **Take measures to protect children from endangering themselves.** Underage users require more privacy protective defaults and other protective measures.	Applicable national laws or regulatory codes may require that users below a certain age be given more private 'privacy protective' defaults and be given information in very clear and simple ways. Children must be prevented from publishing contact details or their exact locations.	This guideline is not about age verifying children, but about helping them to understand the privacy implications of engaging online and how they can protect their privacy. It is also about ensuring defaults for personal profiles for users under age 18 are set to private. Users under 16 should not be able to publish (that is, share with the general public) their exact location or their contact details.
SNS4 **Create appropriate tools to deactivate and delete data from applications and accounts.**	User should be offered the ability to deactivate their account, and must be able to delete their accounts, resulting in complete removal of all personal information and any content posted (from the network and any backend servers).	Protect against malicious actions, and take measures to authenticate users before deactivating or deleting accounts and personal information.

Mobile advertising

Users view their mobile devices as inherently personal, and may have different privacy experiences, expectations and interests to those of 'fixed' online consumers.

While advertising is subject to increasing regulatory and self-regulatory standards over the use of personal information for advertising purposes, studies have shown that giving users insight into how the advertising they see is chosen, and giving users greater control over how they are segmented and profiled, leads them to be more comfortable with and accepting of targeted advertising.

Key to successfully driving mobile advertising and ensuring that ads are relevant and useful to users is establishing best practice based on real transparency and meaningful choice and control.

Guideline	Implementation	Use case and examples
MA1 **Inform users about advertising features.** Let users know when an application is ad-supported before they download and/or activate the application.	Inform users of any intention to place advertising in or around an application. This applies whether or not an application is free to the user.	Many 'apps' are free and are supported by advertising. Users may not be aware of this before they download or activate an 'app'. You could let users know by providing an 'ad icon' and/or a short 'notice'. The icon or notice could link to a URL taking users to more information that helps them understand what information will be used and what choices they have over the advertising. This could help strengthen attitudes towards you and encourage confidence and trust in you and your apps, and your partners or 'app stores'.

Guideline	Implementation	Use case and examples
MA2 **Capture appropriate agreement to target advertising to a user.** Users must agree to targeted advertising and give active consent to profiling across applications or by third parties.	Before you collect any personal information, let users know that advertising will be targeted to them, how and where the advertising will appear, and what information will be used. If an application will build a unique profile of user interests, based on the user's behaviour on the application, and that profile will be used to target advertising, users must be notified that such profiling and targeting will occur and agree to this. Users must be given clear instructions on how to modify or delete a profile and how to **opt out** of profiling and targeting. If the user's profile will be built on activity that occurs outside the scope of one application where users would not reasonably expect a connection between their use of other applications, the user must be informed of the scope of data collected and used for such profiling and must give their active consent. If profiling or targeting will be carried out by a third party (for example, an ad network or mobile analytics company), users must give their active consent to allow the third party to collect and use information in this way.	A user does not need to agree each time and can give consent once. What is important is that the user is given sufficient information and choice to make an informed decision. A user downloads and uses an app called 'coffee2go'. The application collects a range of device data and information about the user's behaviour on the app and creates a profile of that use, with the intention of delivering advertisements based on this single profile information. The user must have actively agreed to this after being told about the profiling and targeted advertising. BUT, the entity responsible for the 'coffe2go' app and for collecting and profiling user information about that app, **also** intends to build a 'combined user profile' that is built on data gathered about the user's behaviour on other applications, such as 'pizza2go'. It is intended to target the user with advertisements based on this 'combined' user profile. The user **must**

Guideline	Implementation	Use case and examples
		be told about this upfront and they must give their active consent before any profiling or targeted advertising can begin.
MA3 **Target based on legitimately collected data.** Advertising may be targeted based only on personal information that is necessary to the application's primary purpose.	Targeting advertising to users based on information collected from the handset (for example, location) or the user's interaction with other apps or with the internet must only use information that has been collected in the course of providing the features and functionality the user has requested.	This allows for applications that are designed to specifically deliver advertising offers to users based on their preferences and interests.
MA4 **Respect privacy when viral marketing.** Viral marketing may only occur with the active consent of the user.	Respect the privacy of users' network of contacts. Applications must not collect information about or send messages to users' contacts without the active consent of the user to participate in any sharing or marketing features an application might include.	
MA5 **Ensure content is appropriate.** Non-targeted advertising must be appropriate to an overall audience The content of advertising must be appropriate to the target age range or known age of the user.	If an application is rated as suitable for younger users, any advertising supplied in or around an application must be appropriate to the minimum age of the rating and target audience and comply with applicable laws, codes or regulations. See also the section on children below.	For example, if an application is rated as suitable for children 7+ then any advertising inserted into the app or placed around the app must be suitable for the minimum age range (e.g. 7 years in this example). The consent of the parent or legal guardian should also be obtained in this example.

Guideline	Implementation	Use case and examples
		Advertising may be subject to specific laws, codes or regulations and which in many cases may prohibit targeted advertising to children.

Location

The use of location data continues to raise significant concerns over user privacy. Location privacy is especially important to mobile users. It is important to ensure users are given opportunities to express real choice about whether their location is accessed and shared by applications.
See also: *Mobile advertising*

Guideline	Implementation	Use case and examples
L1 **Inform the user that location will be used and give them choice.** Applications must only access, use and share location data with a prior and informed agreement.	Location-enabled applications must provide clear notice, before a user's location is accessed or collected , about: • what location data an application intends to access (e.g., cell ID, GPS, village or town) • how the data will be used • whether data will be kept and how long for • who location data will be shared with. If the application will perform a one-time check of a user's active location in order to provide a service requested by a user, and this is the sole purpose of the application, then it is **not necessary to provide the user with further privacy related information or to seek any separate consent**.	If a user downloads or activates an application called 'Where's my nearest ATM' in order that the service can locate the user's device and tell the user about the nearest 'cash point', there is no need to provide the user with additional privacy information or to obtain their active consent (as 'consent' is clear and implicit in the user's request). However, if the application retains location and other contextual information about a user's requests in order to build a profile and target the user with advertising at a later stage, then the application would need to tell the user about this and get their active consent before the user's information is collected and used for these

Guideline	Implementation	Use case and examples
		purposes. See below.
L2 **Capture appropriate consents to use location data.** Some uses of location data require giving users additional privacy information and getting their active consent.	If an application will retain a **history** of a user's location, the user must be told about this and also how long the data will be retained and why. Users must give their active consent to retain a history linked to them as unique individuals and must be able to review and delete the history.	
	If users will receive **advertising** or sponsored results based on contextual location, they must be provided with clear notice that the location application is ad-supported. If users will receive advertising or sponsored results based on the stored history of that user's location, users must provide their active consent.	
	If an application continues to collect, use or share location data during operation of the application or after a user has closed the application: • users must provide active consent to the continued operation of the location feature. • the application must include a means that alerts the user that the location feature continues to operate. • once an application is closed it must not collect location data unless the user has agreed to this. The application must provide easily accessible settings that allow the user to immediately turn	A symbol could be used to indicate that an application is actively accessing a user's location data to enhance the user's awareness and provide the opportunity to actively manage their privacy. Alternatively, users could be sent periodic SMS text messages or alerted via other means that their location is being tracked.

Guideline	Implementation	Use case and examples
	location on or off, including a "location off" feature that overrides all other location settings in the application.	
	If an application will automatically broadcast a user's location or share a user's location with other people, for example, in a **social location** feature: • the default setting must be private. That is, the user must give active consent to begin sharing location and must affirmatively choose individual users or groups of users who will have access to their location. • when sharing has been activated, there must be a clear and prominent indicator that location is being shared. • the user must be able to set the level of granularity of the location (i.e., city, street, exact physical location) • the user must be able to manually override the location information presented or turn off location sharing at any time. • users who are identified or age-verified as children must be prevented from publishing their location (that is, sharing with the general public). If these users are able to share information with their contacts, granularity must by default be set at the city level or wider. If the application shares location data with other applications, sites or services:	

Guideline	Implementation	Use case and examples
	• There must be a disclosure identifying and providing a link or other means to access the application, site or service. • Users must provide active consent to share location with the application, site or service. • User must be able to easily manage what other applications, sites and services have access to the location, for example, to withdraw consent where desired.	

Children and adolescents

While children and adolescents may be skilled at navigating the internet and engaging with mobile applications, they may lack the maturity to appreciate the wider social and personal consequences of revealing their personal information or allowing others to collect and use it.

Applications specifically directed at or used by children and adolescents must ensure that the collection, access and use of personal information is appropriate in all given circumstances and is compatible with national law and any applicable regulatory codes.

See also: *Social networks and social media, Location, Mobile advertising*

Guideline	Implementation	Use case and examples
CA1 **Tailor applications to appropriate age ranges.** Applications that are intended for children and adolescents should be appropriate for the target age range and help such users to easily understand the consequences of installing or using an application or service.	Consider the risk posed to a child or adolescent by the collection and use of personal information and ensure these risks are properly addressed. Ensure that the language and style of the application are appropriate, and that it aids understanding prior to installation and activation of the application. Applications must provide clear notice about the content that will be made available, and its suitability for specific age groups.	
CA2 **Set privacy protective default settings**. Applications that are intended for	Set minimum default settings for categories of personal and location information that pose risks to children and adolescents in relation to the nature of the app.	For example, do not permit the automatic collection and sharing of contact details or location information

Guideline	Implementation	Use case and examples
children and adolescents must have a location default setting that prevents users from automatically publishing their precise location data.	Limit the granularity of location data that a child or adolescent is able to share to a generic level such as city or region.	and limit these to reduce associated risks.
CA3 **Comply with laws on the protection of children.** Applications must at all times comply with the special legal requirements that applicable jurisdictions may impose to protect children.	Specific laws, codes and regulations apply in many jurisdictions to the collection of personal information from children and adolescents. In some cases, parental consent is required before you may collect personal information about children. If your app is directed at children you must take measures to comply with applicable rules relating to the collection and use of their personal information.	
CA4 **Age verify where possible and appropriate.** Under certain circumstances, age verification may be appropriate (for example, where applications contain social networking features or allow access to adult content).	Where possible, integrate age verification processes into the application in order to control access to age restricted apps or content and minimise inappropriate collection and sharing of personal information relating to children and adolescents. Where integration with access controls is not possible, users may be asked to self-certify instead – in that case, they must be asked for a date of birth during installation, activation or registration. Consider that children and adolescents are adept at bypassing safety controls. If users	A date of birth entry form with a prominent disclaimer that users under the age of 16 will be given restricted access will encourage younger users to lie about their age in self-certification.

Guideline	Implementation	Use case and examples
	enter a date of birth indicating an age where they must be denied access to a service or otherwise restricted, they must be prevented from starting over and entering a different date of birth during that session and thereafter if technically possible. Make sure not to include prompts to the user that could be seen as encouraging them to lie about their date of birth.	

Accountability and enforcement

For these guidelines to have an impact, they must apply to all contributors to the mobile application ecosystem and be built by design into the application platform. All involved in the development, provision, sale and supply of applications, who access, collect and use personal information, or who make it possible for others to access, collect and use personal information, must work to create the tools and interfaces that make these guidelines possible.

Guideline	Implementation	Use case and examples
AE1 **Assign responsibility for ensuring end-user privacy is considered and delivered throughout the product lifecycle and through applicable business processes.**	Each entity that collects personal information about users must ensure a company representative (or representatives) is assigned the responsibility for ensuring end-user privacy is built into applications and services and business processes.	
AE2 **Give users tools to report problems regarding an application.**	Users must be able to report problems with applications or the content they contain, or with the application platforms themselves. Users must be provided with information explaining how they can report applications that they suspect, or which are found to breach the privacy and security of their personal information. Procedures should be established and maintained to deal with such reports and address any specific threats and risks.	Provide a short statement and link on the app landing page, and or your corporate website. Clearly signpost this. If you collect email contact addresses (with permission) you could also email that information to users.

For more information contact:

Natasha Jackson
Head of Content Policy, GSMA
njackson@gsm.org

Pat Walshe
Director of Privacy, GSMA
pwalshe@gsm.org

www.gsma.com/mobileprivacy