Mobile Connect Privacy Principles

Version 2.5

11 September 2017

Introduction

Mobile phones and other connected devices are increasingly the main way through which people access the digital world and engage in the digital economy. Mobile identity services play a key role in helping individuals authenticate and manage their digital identities online. Key to realising the potential economic and social benefits of mobile identity services is establishing good privacy practices that foster trust and confidence.

These Principles are intended to guide the use of personal information in Mobile Connect branded services (see www.mobileconnect.io). Mobile Connect enables verified authentication, authorization, identity and attribute solutions from pseudonymous log-in, to consent based attribute verification or validation supporting 'know your customer' purposes, through to helping prevent fraud, and identity theft and account takeover.

The principles are not intended to replace or supersede applicable law or company privacy policies that apply to other non-Mobile Connect practices. The Principles are based on recognised and internationally accepted principles on data protection and privacy and reflect baseline standards expected of organisations that provide Mobile Connect branded services. They broadly describe the privacy outcomes individuals should experience.

Who the Principles apply to

The Principles apply to Mobile Operators and 3rd Party Online Service Providers ('Participating Organisations') that use personal information in Mobile Connect branded services.

➢ Principle 1. Transparency and Notice

Participating Organisations will be transparent with individuals about what personal information is needed and how it will be used in Mobile Connect-enabled services.

Organisations will provide individuals with contextually appropriate and timely *Privacy Notices* that help users make genuinely informed choices, and that are clear and simple and as a minimum provide individuals with the following information:

- the identity of the Participating Organisation (if it's not obvious)
- the main purpose(s) for which the individual's personal information will be used (if it is not obvious)
- to the extent personal information will be shared, who it will be shared with and why (if it is not obvious)
- what choices the individual has about the use of their personal information (see Principle 3)

The Privacy Notice will also provide a hyperlink to a more detailed *Privacy Policy* that describes:

- how Mobile Connect works
- how long personal information will be kept and why?
- name and physical address of the organisation and how individuals can contact it electronically or by telephone with enquiries or concerns about the use of their personal information
- the rights of individuals with regard to the use of their personal information and how they can exercise such rights (See Principle 6)

➢ Principle 2. Purpose and Use Limitations

Participating Organisations will limit the use of personal information to what is necessary to provide Mobile Connect services consistent with Privacy Notices provided to individuals.

Personal information collected for Mobile Connect services may only be used for secondary purposes by providing individuals with clear notice and obtaining their Active Consent (or as otherwise required by law). See also Principle 3 on 'consent'.

➢ Principle 3. User Choice and Control

Participating Organisations will provide individuals with opportunities to exercise appropriate choice, and control over the collection and use of their personal information in connection with Mobile Connect services

Unless obvious from the context clearly explain whether consent is for a specific transaction or whether it will endure for a specific period of time, or until revoked. Explain how individuals can revoke consent once given and provide an easy means for them to do so.

Where feasible, or where required by local law, Participating Organisations should record and retain evidence of active consents given by individuals, and be able to demonstrate such evidence.

➢ Principle 4. Data Minimisation and Retention

Collect and keep the minimum of personal information necessary to provide and support Mobile Connect services (and consistent with Privacy Notices). If you keep an individual's personal information you may be required to provide a copy to the individual on request. See Principle 6 on user rights.

When personal information is no longer required, delete it or render it anonymous.

➢ Principle 5. Data Quality

Participating Organisations will adopt measures to help ensure personal information used for Mobile Connect services is accurate and where appropriate, kept up to date.

Participating Organisations will provide individuals the means to update personal information used in Mobile Connect services (free of charge and in a simple manner).

➢ Principle 6. Respect User Rights – Individual Participation

Trust is key. Be open with and accountable to individuals. Provide them with information about their rights over the use of their personal information and make it easy to exercise such rights. These include:

- how to obtain a copy of any personal information held about them, within a reasonable timescale
- how to have personal information that is inaccurate, or no longer justified, corrected or erased
- how to report and have complaints resolved regarding the use of their personal information

➢ Principle 7. Security

Participating Organisations will adopt appropriate security measures commensurate to the potential for harm to individuals and risks such as the loss, unauthorised access, destruction, use, modification, and disclosure of personal information.

A key aspect of the Mobile Connect service, is that an individual's mobile will be replaced with a unique identifier such as a Pseudonymous Customer Reference (PCR - identifier) in order to protect the privacy of an individual seeking to authenticate and access the services of a 3rd party service provider. Efforts to re-identify an individual's MSISDN or share their personal information may only take place under the following exceptions:

i. with an individual's Active Consent
ii. to provide a service requested by an individual, for the performance of a contract or to assist in the resolution of customer enquiries
iii. where required by law (e.g. a court order or other mandatory obligation)

➢ Principle 8. Education

Provide information about how Mobile Connect identity and attribute services work and ways for individuals to manage and protect their privacy.

Establish internal programmes to educate employees on data protection and privacy requirements and to foster a culture of privacy.

➢ Principle 9. Children and Adolescents

Children and young people may lack the maturity to fully understand the implications of revealing their personal information or allowing others to collect and use it.

When Mobile Connect services are directed at, or intended for, children and young people Participating Organisations will:

- use language and style that helps children and young people easily understand what is being asked and that helps them make informed decisions about the use of their personal information.
- comply with applicable national laws and any special legal requirements, including age verification laws.

➢ Principle 10. Accountability

To generate confidence and trust in the effectiveness of these principles, Participating Organisations will, as a minimum:

- establish policies, procedures and practices to help ensure compliance with the Principles
- where a Participating Organisation relies on another Participating Organisation to collect consent to verify, validate or otherwise disclose identity attributes it holds about an individual, both organisations will establish transparency, notice and consent standards, and contractually bind each other to meet such requirements in a 'trusted service provider relationship'
- establish mechanisms for individuals to report complaints and incidents regards the use of their personal information and that aid the investigation and remediation of such complaints

Definitions and terms:

Active Consent: means an individual is given a clear and prominent opportunity to agree a specific and notified use of their personal information.

Personal Information: includes, but is not limited to data that could be used to identify, locate or contact an individual. Personal Information may include:

- data collected directly from an individual (e.g. entered by the user via an application's user interface and which may include name and address, email address, passport details, credit card details)
- data obtained indirectly (e.g. mobile phone number, gender, birth date, location data, IP address, IMEI, unique phone ID)
- about an individual's behaviour (e.g. location data, service and product use data, website visits)
- held on an individual's device (call logs, messages, user-generated images, contact lists or address books, notes, and security credentials)

Pseudonymous Customer Reference (PCR)[1]: is a unique identifier that replaces an individual's mobile phone number and that may be used to distinguish one individual from another. Participating Organisations may only re-identify or capture an individual's mobile phone number under the exceptions listed in Principle 7.

1 A PCR is used during Step 1 of Mobile Connect to uniquely authenticate an individual and map them to specific service provider accounts without revealing their identity and without individual's being required to disclose personal information. The PCR allows individuals to remain anonymous to participating organisations until such time that specific actions are taken to directly identify individuals by association to the PCR. In simple terms, the PCR is assigned and used to recognise but not identify individual users.