Privacy Code of Conduct on mobile health apps

The Privacy Code of Conduct on mobile health (mHealth) apps, facilitated by the European Commission, will provide a competitive advantage for those who are signatory to it, and help to promote trust among users of mHealth apps.

The Code of Conduct for mHealth apps was submitted by the drafting team to the Article 29 Working Party on 7 June 2016. After reviewing the Code, they will issue an opinion which is crucial before the Code is
applied in practice. After the entry into application of the General Data Protection Regulation in May 2018, additional approval would also be sought by the European Data Protection Board.

The European Commission has acted as a facilitator, provided legal and policy expertise and oversaw the development of this work and provided resources.

Main provisions for app developers

The core of the Code of Conduct consists of practical guidelines for app developers. The most relevant elements of this section are the following:

- **User's consent**: The user's consent for the processing of personal data must be free, specific and informed. Explicit consent needs to be obtained for the processing of health data. Any withdrawal of consent has to result in the deletion of the user’s personal data.

- **Purpose limitation and data minimisation**: The data may be processed only for specific and legitimate purposes. Only data that are strictly necessary for the functionality of the app may be processed.

- **Privacy by design and by default**: The privacy implications of the app have to be considered at each step of the development and wherever the user is given a choice. The app developer has to pre-select the least privacy invasive choice by default.

- **Data subjects rights and information requirements**: The user has the right to access their personal data, to request corrections and to object to further processing. The app developer needs to provide the user with certain information on the processing.

- **Data retention**: Personal data may not be stored longer than necessary.

- **Security measures**: Technical and organisational measures need to be implemented to ensure the confidentiality, integrity and availability of the personal data processed and to protect against accidental or unlawful destruction, loss, alteration, disclosure, access or other unlawful forms of processing.

- **Advertising in mHealth apps**: There is a distinction between advertising based on the processing of personal data (requiring opt-in consent) and advertising not relying on personal data (opt-out...
- **Use of personal data** for secondary purposes: Any processing for secondary purposes needs to be compatible with the original purpose. Further processing for scientific and historical research or statistical purposes is considered as compatible with the original purpose. Secondary processing for non-compatible purposes requires new consent.

- **Disclosing data to third parties** for processing operations: The user needs to be informed prior to disclosure and the app developer needs to enter into a binding legal agreement with the third party.

- **Data transfers**: For data transfers to a location outside the EU/EEA, there needs to be legal guarantees permitting such transfer, e.g. an adequacy decision of the European Commission, European Commission Model Contracts or Binding Corporate Rules.

- **Personal data breach**: The Code provides a checklist to follow in case of a personal data breach, in particular the obligation to notify a data protection authority.

- **Data gathered from children**: Depending on the age limit defined in national legislation, the most restrictive data processing approach needs to be taken and a process to obtain parental consent needs to be put in place.

### Structure of the code of conduct

The **Code of Conduct** is divided into several sections, which are:

1. **About the Code**
2. **Practical Guidelines for app developers**
3. **Annex I – Privacy Impact Assessment**
4. **Annex II – Information notices**

The first section introduces the topic and explains the purpose and scope of the Code of Conduct. It targets mobile apps which process data concerning health, the definition of which is further explained in the text. This section also addresses the governance of the code and explains the organisational framework to support it, which includes a mechanism to enforce the Code and monitor its compliance as well as provides a model for its sustainability.
The Code also contains two Annexes:

1. **A Privacy Impact Assessment** which is intended to help app developers determine whether they have respected the main requirements of the Code, and whether they have followed good privacy practices before making the app available;

2. An example of an **information notice**.

A three-tiered multi-stakeholder governance model is foreseen with the following bodies:

- **General Assembly**: a consultative organ and the one ensuring financial stability. Composed by representatives of app developers, the data protection community, industry associations and end-users.
- **Governance board**: organ with decision making powers and responsible for the maintenance, interpretation and evolution of the Code appointed by the General Assembly.
- **Monitoring body**: in charge of monitoring compliance and enforcing the Code in accordance with the requirements of the General Data Protection Regulation with the required level of expertise and independence. It will be appointed by the Governance board.

**Background leading to drafting of the code**

The European Commission's 2014 mHealth Green Paper consultation revealed that people often do not trust mHealth apps because of privacy concerns. Respondents considered that having users' consent as well as strong privacy and security tools in place is a crucial issue for mobile health apps.

The European Commission encouraged setting up a code of conduct on mobile health apps, covering privacy principles, to increase trust. The Code provides practical guidance for app developers on data protection principles while developing mHealth apps. App developers respecting the rules of this code will be able to sign it and their apps will be included in a publicly available register.

Work on the Code of Conduct started in April of 2015, when a drafting team of industry members was set up with the objective of developing the text of the code. This drafting team (consisting of the App
Association (ACT), App developers Alliance, Apple, COCIR, DigitalEurope, DHACA, ECHA, EFPIA, Google, Intel, Microsoft, Qualcomm and Samsung) worked through regular conference calls and face-to-face meetings.

The European Commission launched a call for interest to find an editor for the code. Since August 2015, this editor has been supporting the drafting, acting as a rapporteur of the drafting team, and solving difficult issues that caused lack of consensus.

Early drafts of the code were presented at different stakeholder events giving interested parties the possibility to make comments.

The Code has been drafted with the vision to ensure it to be easily understandable, also for SMEs and individual developers who may not have access to legal expertise.

The possibility of drawing up codes of conduct is foreseen in Article 27 of the Data Protection Directive. This possibility continues to exist under the General Data Protection Regulation (in Article 40) where codes of conduct will have an even more important role.

The Article 29 Working Party has the possibility to approve codes of conduct submitted to them which gives them more legitimacy. This task will be taken over by the European Data Protection Board, set up under the General Data Protection Regulation. Codes approved by the European Data Protection Board can furthermore be granted general validity in the European Union by an implementing act.

Read the whole text of the Code of Conduct

Refer to the whole drafting process:

- Meeting 12 May 2015
- Meeting 6 July 2015
- Meeting 7 December 2015

Team responsible

DG Connect

Published:
Tuesday, 23 May, 2017
You may be interested in

An overview of eHealth studies

mHealth

eHealth

Interoperability & standardisation: connecting eHealth services

Transatlantic Cooperation

Virtual Physiological Human

Managing Health Data

Telemedicine

Benefiting from personalised care