Draft Code of Conduct on privacy for mobile health applications

I. About this Code

1) Introduction

Mobile health applications have a clear potential to bring significant benefits to individual citizens and to society as a whole. Citizens can benefit from continuous and readily accessible support in monitoring, evaluating and improving their health. Society as a whole not only benefits from having a healthier population, but can also gain new knowledge and develop new services and applications on the basis of the data processed via these apps.

However, data concerning health is highly privacy sensitive. Therefore, mobile health apps must be designed in such a way that the privacy of the end users is optimally protected. Similarly, these apps have the potential to empower users, provided that: the users receive sufficient insight into the functioning of the app, and are able to assess more easily which of the many apps on the market meet their privacy concerns. This Code has been developed with these goals in mind: it provides an accessible and effective tool to ensure that mobile health apps have been properly developed, and that they can be entrusted with data concerning health in a manner that complies with European legal principles of data protection law.

2) Purpose

The purpose of this Code of Conduct (hereafter the 'Code') is to foster trust among users of mobile applications (hereafter 'mHealth applications' or 'mHealth apps') which process personal data that includes data concerning health. mHealth apps must provide users with clear and prominent information about how their data will be used to help them make informed decisions prior to using an app. This will help ensure data are used in a fair and transparent manner, which is crucial for fostering trust. The Code thus aims to facilitate data protection compliance[1] and to promote good practices in this field.

The Code aims to achieve this goal by providing specific and accessible guidance on how European data protection legislation should be applied in relation to mHealth apps. This guidance is specifically targeted towards app developers, i.e. individuals, companies or organisations who make available (either directly or via application stores) software applications for mobile devices that are intended to process data concerning health. This focus on app developers (rather than e.g. on app programmers or application stores) is due to the consideration that app developers design and/or create the software which will run on the smartphones and thus decide the extent to which the app will access and process

[1] Other compliance issues which are not addressed by this Code include topics such as compliance with medical devices legislation, consumer protection law, and e-commerce legislation. Compliance with this Code does not guarantee compliance with these separate frameworks and vice versa.

the different categories of personal data in the device and/or through remote computing resources[2]. The Code aims to assist them in making responsible and informed choices that comply with European data protection law.

In the context of this Code, "personal data" includes information on the user (such as their name, address, or contact information), device identifiers, location data, and any other information relating to an identified or identifiable natural person. "Data concerning health" should be understood as any personal data related to the physical or mental health of an individual, including the provision of health care services, which reveal information about his or her health status[3].

The context of processing, and particularly the purpose for which the app is made available or whether the data is made available through the app to a member of the medical community, is however also relevant to determine whether data should be qualified as data concerning health. Data concerning health also includes any personal data that has a clear and close link with the description of the health status of a person[4]. This includes raw sensor data that can be used in itself or in combination with other data to draw a conclusion about the actual health status or health risk of a person, and the conclusions themselves.

Mere lifestyle data, for instance if they are raw data on an individual's habits and behaviour that do not inherently relate to that individual's health, are not necessarily considered as data concerning health. Lifestyle data can however be qualified as data concerning health when they have a clear and close link to the person's health status.

By way of examples:

> **E.g.** an app allows a user to track whether she has taken her prescribed medications and thus complies with the advice provided by her doctor. **This app processes data concerning health**, since the consumption of medication is indicative of the health of an individual.
> **E.g.** an app tracks footsteps solely as a way of measuring the users' sports activities during a single walk. The data is not stored by the app developer to create a profile that evaluates the user's physical fitness or health condition, nor is it combined with other data. **This app does not process data concerning health**, since this is merely lifestyle data.

However, **if the data is also used to measure or predict health risks** (e.g. risk to injury or heart attacks) **and/or stored in order to analyse and evaluate the user's health**, **then the app does process data concerning health**. For the avoidance of doubt, the distinction between data concerning health and other types of personal data does not determine whether data protection law applies. Data protection

[2] As confirmed by the Article 29 Working Party Opinion 02/2013 on apps on smart devices; see http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf

[3] For more detailed guidance on this concept, we refer to the guidance provided by the Article 29 Working Party in its letter of 5 February 2015 and its related Annex; see http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_annex_en.pdf ; and to the ruling of the European Court of Justice in the matter of Lindqvist (C-101/01, Slg. 2003, I-12971, No. 50)

[4] As noted in the Article 29 Working Party's Working Document on the processing of personal data relating to health in electronic health records; see http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2007/wp131_en.pdf p. 7

law must be respected whenever any type of personal data is processed. This Code however targets data concerning health in particular, as this is a particularly sensitive category of personal data that relates to one of the most intimate aspects of our lives: our health. As such, it is subject to more stringent legal requirements. It should be noted that additional legal obligations can apply to more specific types of personal data, such as biometric data[5] and genetic data[6]. If the mHealth app processes such types of personal data, the app developers should familiarise themselves with additional legal requirements first.

The requirements of this Code have been drafted in a pragmatic and accessible manner, to ensure that SMEs and individual developers – who may not have systematic access to expert legal advice – can also benefit from its guidance. None the less, the Code should not be seen as a substitute for qualified legal advice.

App developers may also choose to publically declare their compliance with the Code. By doing so, they confirm that they comply with all requirements of the Code, and that they will continue to comply with them for any data relating to health collected by them (if any) while their declaration was in effect. In this manner, users will be able to determine more easily which app developers have taken particular steps to ensure that their personal data is processed in a secure and trustworthy manner.

3) Scope

This Code of Conduct applies to app developers as described above. This can include individuals and companies, private and public sector organisations, for-profit and not-for-profit organisations. For the purposes of this Code, it is not relevant whether the app developers have programmed the apps themselves or whether they have outsourced (part of) the development process. Similarly, it is not decisive whether the data concerning health remains on the device or whether it is transferred to an external data store (although the obligations of an app developer are of course very different in both scenarios). This Code can be applied by any app developers as defined above.

It is worth noting that the direct applicability of European data protection law to app developers can be strongly affected by design choices when the app was created. Specifically, if an app developer does not exercise any control over the processing of personal data through the app and does not use the outcome of the processing - which will commonly be the case if no personal data is ever sent to the app developer or to another third party by the app – then the app developer will in principle not fall directly within the scope of applicability of European data protection law. App developers should at any rate take care to ensure that their app is well designed, secure, and satisfies their user's legitimate privacy expectations. For that reason, the current Code takes a broad approach, and an app developer can also use it to assess and declare the compliance of its app with this Code, irrespective of where personal data is stored or otherwise processed.

[5] Defined as any personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of an individual which allows or confirms the unique identification of that individual, such as facial images, or dactyloscopic data.

[6] Defined as all personal data relating to the genetic characteristics of an individual that have been inherited or acquired, which give unique information about the physiology or the health of that individual, resulting in particular from an analysis of a biological sample from the individual in question.

4) Adherence to the Code & governance

Principles for a multistakeholder governance model

This Code of Conduct has been drafted based on inputs from a wide range of stakeholders, containing representatives with expertise in data protection, self- and co-regulation, ICT and health care. This multistakeholder approach is a key element of the Code's genesis, which should also be reflected in its future governance, as it allows the Code to effectively address its four distinct audiences: app developers, the data protection community, industry associations, and of course the end users of the apps[7].

These audiences each have a different role in the Code, although they share the common objective of enabling and offering safe and trustworthy mHealth apps for the market, for which this Code can be a crucial tool. Therefore, the governance principles set out in this chapter strive to create a sustainable model that encourages participation of all relevant stakeholders, through neutral and credible governance mechanisms that allow the Code to be maintained, applied and enforced with the interests of each stakeholder group in mind.

Simple, representative and autonomous

Drawing on the rules and principles of the current Data Protection Directive and the General Data Protection Regulation, the Code will be governed in accordance with the following governance structure:

- A **General assembly** will be established, which is comprised of representatives of all the stakeholders mentioned above - app developers, the data protection community, industry associations, and end users of the apps (as represented e.g. via civil society, consumer protection associations, and/or patient associations). The General assembly will meet at least twice a year to provide inputs, suggestions and criticisms for the maintenance, interpretation and evolution of the Code. The General assembly is the consultative organ that supervises the governance of the Code, but which has no day-to-day operational tasks or decision making power. Initially comprised of all members of the drafting team of the Code of Conduct, aspiring new members may submit an application to join to the Governance board (see below), who will decide to accept or reject applications. The General assembly will also provide financial stability of the Code through annual financial contributions from its members, which will take into account the scale and nature of their activities. This ensures the continued involvement and representation of the interests of each stakeholder group.
- Decision making powers for the Code will lie with a **Governance board.** Board members will be selected from among the General assembly members: after a member of the General assembly has presented their candidacy to become a member of the Governance board, the General assembly will decide by a majority vote whether the member is accepted or not. The Governance board will contain representatives from app developers and app developer associations, as well as other industry associations (including the ICT industry and health care professionals. To ensure its effectiveness, it is envisaged that the Governance board will

[7] As represented via consumer organisations, patient associations, etc.

comprise 6-10 members. The Governance board will take decisions on the maintenance, interpretation and evolution of the Code, and on membership of the General assembly, based on the inputs from the General assembly. The multistakeholder composition of the group and the interaction with the broader General assembly will protect the Code against bias and conflicts of interest.

- It is however not envisaged that either the General assembly or the Governance board will perform operational tasks, including the enforcement of the Code, since this would entail a risk of conflicts of interest. Instead, operational tasks will be entrusted to a **Monitoring body** meeting the requirements of the General Data Protection Regulation[8]. This Monitoring body will be appointed by the Governance board after consultation of the General assembly, and will be entrusted with such tasks as the management of a Code specific website (targeting developers and the public separately, using language which is appropriate to each of them), facilitating communications with the public, and monitoring compliance in accordance with the requirements of the General Data Protection Regulation and as set out below.

This three tiered structure ensures compliance with all legal and operational requirements for the operation of a code of conduct: it ensures that the Code is driven by associations and other bodies involved in the mHealth ecosystem, it comprises multistakeholder involvement to ensure that all relevant voices can be heard, and it foresees a clear separation between the stakeholders of the Code (General assembly), the management of the Code (Governance board), and the operational tasks including monitoring of compliance (Monitoring body).

While these bodies have currently not yet been set up, the stakeholders who have participated in the creation of the Code have expressed their interest and willingness to participate in the establishment of a governance structure as set out above. Collectively, they have the expertise required to perform these functions as needed.

Credible governance and enforcement

A Code of Conduct must be capable of monitoring compliance with its provisions and of taking enforcement action where necessary. The current Code will meet this requirement through the following enforcement mechanisms:

- All app developers who wish to declare their adherence to the Code will need to submit a completed privacy impact assessment as contained in Annex I of the Code (or any other PIA which provides at least the same information and the same level of transparency) and a self-declaration of compliance to the Monitoring body. This PIA and declaration will be subjected to a summary check of their completeness (have all questions been addressed?) and credibility (are the answers plausible?) by the Monitoring body. If they are found to be acceptable, the app developer and its app will be identified in a centralised public register, maintained by the Monitoring body.
  The app developer will thereafter be required to ensure the continuous accuracy of the declaration, making any required updates as necessary. If it cannot or will not ensure the continuous accuracy of the declaration, the app developer may choose at its own discretion to withdraw the declaration at any time, thereafter also ensuring that it no longer communicates its adherence to the Code.

[8] Specifically, as set out in Articles 40.4, 41.1 and 41.2 of the General Data Protection Regulation

- On a voluntary basis, the app developers whose declaration has been accepted may also choose to undergo a third party audit and certification of their compliance with the Code. Certifications will be done at the app developer's own expense, and can be done by any party or organisation mandated by the Governance board to conduct such audits.
- On a rolling basis, the Monitoring body will randomly select a sample of the accepted declarations for re-checking of their continued adherence, using at least the same standards as under the initial declaration (including re-auditing for app developers that have undergone an audit). This will allow noncompliance to be detected and addressed even in the absence of complaints.
- Furthermore, the Monitoring body will implement an alternative dispute resolution and complaints handling process where any member of the public can lodge complaints against app developers adhering to the Code, in which an independent panel of experts (a Complaints panel) will make decisions to settle such disputes. The Complaints panel will process complaints, establish whether violations of the Code have occurred and decide on possible sanctions and remedies. Panel members will be appointed by the Governance board, thereby protecting against conflicts of interest.
- Finally, the Monitoring body will regularly inform competent national data protection authorities on any complaints received, the outcomes of dispute resolution processes, and the declaration and PIA provided by the app developer.

After publication in the Code's registry, the app developer may apply any trust mark made available for this purpose to the related app, under the terms and conditions as set by the Governance board.

If the app developer is found to be in breach of the Code (as a result of a random check, a complaint, or a decision from a competent court), the relevant declaration from the app developer will be voided. The Monitoring body will thereafter mark the affected app as having failed the adherence requirements. The app developer will be forbidden to make reference to the Code or to use any trust mark in any of its documentation or publications in relation to the app, including its website.

II. Practical Guidelines for app developers

1) How should I obtain the consent of the users of my app?

Prior to or as soon as users install your app, you must obtain their free, specific and informed consent in order to process their data for the purposes you've described to them. The consent to process data concerning health must be explicit (i.e. require a clear and unambiguous action from the user); it is not sufficient that they don't protest after having been informed of your intended use of their data. Furthermore, you must be able to demonstrate that users have provided their consent.

Consent should be obtained using the most effective means to communicate with users. Granular and contextual consent, in which consent is sought during various stages of the use of the application, with additional consents being sought when the app processes the user's data

in a new manner, can be considered a good practice if this permits the user to exercise better or more effective control over his or her personal data. Thus, consents can be obtained when installing it or at various times during use, as long as consent is obtained before processing begins. It should be noted that processing of data for historical, statistical or scientific purposes can be permissible even when this is not specifically authorised by the user's consent, provided that specific legal safeguards are applied; this is addressed under question 7 below.

Similarly, users must be able to withdraw their consent using accessible and easy to understand mechanisms, including e.g. by choosing to delete their personal data (locally or remotely, or both), or by choosing to uninstall the app. Any withdrawal of consent should result in the deletion of the user's data from any systems under your control, unless the users have consented to your retention of their data.

Note that consent requires that users have been provided with clear and comprehensible information first. Key information shall not be embedded in lengthy legal text, and shall be presented in a clear, user-friendly manner.

2) **Which are the main principles that I must respect before making an mHealth app available?**

Purpose limitation

Your mHealth app must be designed to only collect and process data concerning health for specific and legitimate purposes. These purposes must be clearly defined before any data processing takes place, and must bear a meaningful relationship to the functionality of the app.

This is an important assessment: once your purposes have been decided and clearly communicated to the user, the app may only process the data for compatible purposes – with the consent of the user and as required for the functionality of the app – as long as you assess the compatibility on a case by case basis considering:

- the relationship between the initial purpose and the purpose for further compatible processing;
- the context of collection and the expectation of the user;
- the sensitivity of the data and the impact on user of the further processing;
- the safeguards that you've implemented to prevent any undue impact on the user.

E.g. an app that monitors blood sugar concentration levels to assist diabetes patients in dispensing medication, may not also sell this information to vendors of medication. The commercial exploitation of data concerning health by third parties is not compatible with the original purpose of providing assistance to diabetes patients.

If the personal data is to be used for a purpose other than the initial or compatible purpose of collection, the personal data must either be completely anonymised[9] before re-using it (removing any possibility to identify an individual on the basis of the data), or alternatively the free, informed and explicit consent of the users with the new use must be obtained. In either case, you must notify the user of any change in purpose of the data collected.

Data minimisation

You must carefully consider what data is strictly necessary for your app to provide its desired functionality, in line with the purposes you described. Do not collect or process more data or for a longer duration than strictly necessary.

> **E.g.** You should not store exact date of birth when a generic age (or age bracket, such as age 25-35) is sufficient for your app to function correctly.

Transparency – information to the users

You must provide users of your app with a clear description of the purposes for which their personal data will be processed. The description must allow them to understand what personal data (including specifically data concerning health) is collected about them and why. Make sure that the language is understandable to your intended users. The third question below (3. What information shall I provide to the users before they can use my app?) provides further requirements on the information you should give.

Privacy by design and privacy by default

Privacy by design[10] means that the privacy implications of your app and its use have been considered at each step of its development, and that you've made design and implemented choices that will support the privacy of your users wherever possible.

> **E.g.** You must consider whether you've appropriately minimised your use of personal data, and what kind of security measures are required to avoid accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, the user's data. It's much more effective to implement these measures directly rather than implementing them as an add-on.

[9] For guidance on this topic, see the Article 29 Working Party Opinion 05/2014 on Anonymisation Techniques; see http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

[10] More formally, privacy by design can be defined as a requirement to "*implement technical and organisational measures appropriate to the processing activity being carried out and its objectives, such as data minimisation and pseudonymisation, in such a way that the processing will meet the requirements of this Regulation and protect the rights of data subjects*", "*having regard to available technology and the cost of implementation and taking account of the nature, scope, context and purposes of the processing as well as the likelihood and severity of the risk for rights and freedoms of individuals posed by the processing*."

Privacy by default[11] means that, wherever the user has a choice with respect to the processing of his or her data but does not take any action to express a preference, by default the app developer has pre-selected the least privacy invasive and compliant choice.

> **E.g.** If your app allows users to share their data (e.g. by publishing it on a social network), by default this option must be switched off. Users should be required to actively consent to using these options.

Where possible and beneficial to the users, app developers should help users in making meaningful and granular choices by allowing them to use or decline specific uses of the application as preferred, rather than obtaining a single consent that covers all possible uses.

> **E.g.** Your app can support privacy by design by allowing users to easily review and change the app settings after installation.

Data subject rights

The users of your app have the right to access any personal data relating to them that you have stored. Furthermore, they have the right to obtain corrections to this data if it is incorrect, and to object to any further processing (including by demanding the deletion) of any data you have stored in relation to them. These rights do not apply if the app developer factually cannot access, change or delete the personal data (e.g. because it is stored on the user's device without any means of the app developer to exercise control over the data), and the user is given the option of undertaking the required actions herself. You should familiarise yourself with applicable laws in relation to these rights[12], and respect these at all times.

Your app should implement user friendly interfaces in your app that facilitate the exercise of these rights. Users should be able to easily find all relevant information in relation to their rights.

3) **What information shall I provide to the users before they can use my app?**

As noted above, the users should be given a clear description of the purposes for which their personal data will be processed. You must also identify yourself clearly and unambiguously, and provide contact information that will allow users to raise any questions that they may have in relation to their privacy protection in your app or to exercise their rights to access, correct and

[11] More formally, privacy by default can be defined as a requirement "*to implement appropriate measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed; this applies to the amount of data collected, the extent of their processing, the period of their storage and their accessibility. Where the purpose of the processing is not intended to provide the public with information, those mechanisms shall ensure that by default personal data are not made accessible without human intervention to an indefinite number of individuals.*"

[12] You should in particular consider whether your app may also be covered by patients' rights legislation, and/or by legislation in relation to clinical trials, or other laws that may affect the data subject rights.

delete their data, and their right to data portability (i.e. the right of the user to obtain any personal data related to them that they have entrusted to the app, in a structured, commonly used and machine-readable format; and the right of the user to transmit those data to another app). Users must also be made aware in clear and plain language whether any data concerning health will be stored in any location other than their device.

Users must be able to easily find this information again at any time after installing your app.

It can be challenging to provide your users with sufficient and useful information without overloading them with too many details. For this reason, a layered approach is recommended where users first receive a condensed notice in which they receive the most crucial information, and have the possibility of clicking through to a full privacy policy in which all other relevant elements are contained[13].

The essential scope of information about data processing must be available to the users before app installation. Secondly, the relevant information about the data processing must also be accessible from within the app, after installation.
To generate effective notices and to integrate them into your app, you may wish to use existing notice generators. Examples include:

- The Intuit Mobile Privacy Notice Code, consisting of open source code that you can integrate into your app; click here.
- The MEF Mobile Policy Generator; click here.

The condensed notice shall:

- Identify you, the app developer;
- Briefly describe the purpose of the data processing, and how the data will be used and fits in your products and services, in order to guarantee fair processing in respect of the app user);
- Indicate the precise categories of personal data that the app will process;
- Indicate whether personal data will be transferred from the user's device, and if so, to which recipients or categories of recipients of the data;
- Inform the user of their right to access and correct personal data, and to delete it
- Inform the user that their use of the app is strictly voluntarily, but requires their consent to permit the processing of personal data.
- Provide contact information where the user can ask data protection related questions.
- Contain a link to a full privacy policy.

To further assist you in drafting a condensed notice and a full privacy policy, examples can be found in Annex II. Note however that it is not recommended to simply copy these into your app;

[13] For more information on these concepts, see the Article 29 Working Party's Opinion 10/2004 on More Harmonised Information Provisions;
http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp100_en.pdf

you must review carefully which changes are needed to ensure they apply to your app, and **make the necessary updates**.

4) How long can I keep the data?

You may not store any personal data, including data concerning health, longer than necessary for the functionalities of the app, unless this is required or permitted by law. Clear criteria must be set for the deletion of data, and these must be clearly communicated to the user, along with the consequences.

E.g. after a certain period of time of non-use of the app, data should be considered expired and must be deleted, even if the user takes no action to do so herself. At any rate data must be deleted when it is no longer relevant for the functionalities of the app.

Extended periods of retention shall only be used when continued retention is necessary for the purposes outlined to the user.

Instead of deletion, you may also choose to irreversibly anonymise data. Note however that this can be very challenging for data concerning health: it must be practically impossible for anyone to link the data to any individual. Furthermore, you should be aware of the risk of re-identification: if the data could be de-anonymised and relinked to a natural person by combining it with other information, it should still be treated as personal data, rather than as anonymous data.

When the app is uninstalled from a device by the user, users should be asked whether they want to delete their personal data, either locally or remotely, or both.

5) Do I have to implement any security measures?

App developers should ensure the confidentiality, integrity and availability of the personal data processed via their apps. If personal data is processed by or on behalf of the app developer, then the app developer is required under applicable data protection law to implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction, loss, alteration, disclosure, access and other unlawful forms of processing.

Appropriateness of security measures is highly dependent on the nature of the data and its potential impact on the user. The app developer should ensure that the app is designed in accordance with existing guidance on secure smartphone app development[14] and secure software development[15].

[14] See e.g. the guidance provided on this topic by ENISA: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-applications/smartphone-security-1/smartphone-secure-development-guidelines/at_download/fullReport

[15] See e.g. the guidance provided on this topic by ENISA: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-applications/secure-software-engineering

In order to determine which measures are appropriate for a specific app, app developers must assess the personal data processing activities within their app, identify possible data protection risks, and take appropriate mitigating measures. This requires the implementation of a sustained risk management process, in which risks to the protection of personal data are assessed and re-evaluated frequently, in order to ensure that the app continuously provides security assurances that are appropriate for the risks involved.

As a complement to this risk assessment process, app developers must conduct a Privacy Impact Assessment to that end. To facilitate this process, a template for the Privacy Impact Assessment is provided in Annex I of the Code.Furthermore, when conducting the Privacy Impact Assessment, the app developer must consider the following objectives:

- The app shall adhere to the principles of privacy by design[16] and privacy by default;
    - E.g. you should consider if data can be pseudonymised or anonymised without impairing the app's functionality; when doing so, a risk assessment should be conducted, taking into account all available data, services, and partners with whom data could be exchanged, in order to mitigate the risk of re-identification;
    - E.g. you should consider whether you can build appropriate authorisation mechanisms into the app to avoid, detect and/or log unlawful access.
    - E.g. you should consider whether you can use effective encryption both for locally stored personal data, for data in transit between the device and your own servers, and for remote storage on your servers, to further mitigate the risk of breaches.
    - E.g. you should consider whether regular, independent system security audits may be required or advisable, in the light of the apps potential impact on your users (e.g. considering the highly sensitive nature of the data, the scale of your user community, or the potential consequences of its use to the health and safety of your users;
    - E.g. you should consider whether the app needs a notification mechanism to inform users when an updated version of the app is available;
- The app should be tested using mock data prior to making it available to real end users;
- If personal data is processed by you or on your behalf, you should ensure that incidents can be identified followed up appropriately.
    - E.g. Internal incident monitoring, reporting and management procedures can be implemented, along with breach notification processes.

6) Can I show any advertisements in an mHealth app?

The sustainability of apps in general (including mHealth apps) is often supported by some form of advertising. This is permissible from a data protection perspective[17] under the following conditions:

[16] See other technical mechanisms to implement privacy by design at https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-and-data-protection-by-design and the GSMA Privacy Design Guidelines for Mobile Application Development at http://www.gsma.com/publicpolicy/privacy-design-guidelines-for-mobile-application-development

- The use of advertisements must be clearly authorised by the user before the app is installed.
- If the app uses contextual advertisements which are shown to the app user without sharing any personal data with any third party (such as an ad network) and without any processing of data concerning health which is specific to that individual user, then the user must be given the option to opt-out of the contextual advertising before any data processing for this purpose takes place.

  E.g. an app that monitors blood sugar concentration levels to assist diabetes patients shows advertisements which are relevant specifically to diabetes patients. The advertisements are placed without any form of processing of data concerning health related to the individual users, i.e. the blood sugar measurements are not used to target the advertisements specifically. In this case, an opt-out right for the users to such contextual advertising at the time of installation is sufficient.

- If these conditions are not met (i.e. because the advertising is provided by a third party that receives the app user's personal data, or because it involves the creation of user profiles across multiple apps and services, or because data concerning health is processed to target the advertisements), then the prior opt-in consent of the user must be obtained[18]. This consent must be obtained specifically and separately, i.e. it requires an explicit action of the user separate from his/her consent to install and use the app (e.g. checking a box) that confirms their consent on this point.

  E.g. an app that monitors blood sugar concentration levels to assist diabetes patients shows advertisements provided through an ad network which has received personal data in relation to the ad user. In this case, opt-in consent is required.

It is permissible for the app to make acceptance of advertisements a condition of the use of the app, i.e. exercising the opt-out right may result in the removal of the app from the user's device.

In order to facilitate the exercise of choices by the app user, the app developer should take notice of existing guidelines, practices and services to support data protection compliant online advertising services. This includes any guidance and recommendations provided by data protection authorities[19] and choice management services[20].

---

[17] It should be noted that the lawfulness of advertisements can also be impacted by other legislation. National rules will likely apply to advertisements for medications and/or medical devices, and advertisements provided via the app will need to respect any regulations in relation to online marketing.

[18] As confirmed by the Article 29 Working Party Opinion 02/2013 on apps on smart devices, p. 10 and 13; see http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf

[19] Such as the Article 29 Working Party Opinion 2/2010 on online behavioural advertising; see http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf

[20] Such as YourOnlineChoices; see http://www.youronlinechoices.com

7) Can I use personal data collected via my mHealth app for secondary purposes, e.g. for 'big data' analysis?

Any processing of personal data must be compatible with the purposes for which you originally collected the personal data, as communicated to the users of your app. Secondary processing of the data for scientific and historical research purposes or statistical purposes (assuming that these purposes were not originally communicated) is however still considered as compatible with original purposes if it is done in accordance with any national or EU level rules adopted for such secondary processing.

This means that, in order to process data for such secondary purposes, you will need to determine which national or EU level laws apply, and respect any restrictions. This implies that you will need to minimise any data collection, including by anonymising data wherever possible, or by pseudonymising it[21]. Processing of non-anonymised and non- pseudonymised data for historical, statistical or scientific purposes should only be done if there are no other options. You should take into account existing best practices[22], or any guidelines available from national data protection authorities.

Please also note that the special regime applies only to processing for historical, statistical or scientific purposes, and that other legal regimes than data protection rules – such as e.g. rules on clinical trials and deontological rules requiring the involvement of ethical committees[23] – may apply. Any big data analysis or other type of secondary processing that falls outside of this context (e.g. big data analytics for market research purposes, or communication of data concerning health to insurance companies or employers) is subject to normal data protection rules, and will thus require you to ask for new prior consent after informing the users of your intentions.

8) What shall I do prior to disclosing data to a third party for processing operations?

It is possible that you need to make personal data available to a third party, either to provide purely technical services (e.g. in order to maintain backups with a third party), or for substantial processing (e.g. to analyse data concerning health collected via the app). A few general rules apply, irrespective of your reasons for making data available to a third party.

You may only make personal data available to a third party for processing operations after you have appropriately informed the user.

[21] For guidance on this topic, see the Article 29 Working Party Opinion 05/2014 on Anonymisation Techniques; see http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

[22] Such as the ETRIKS Code of Practice on Secondary Use of Medical Data in Scientific Research Projects; see http://www.etriks.org/wp-content/uploads/2014/12/Code-of-Practice-on-Secondary-Use-of-Medical-Data-with-recognition.pdf

[23] Such as Regulation No 536/2014 of the European Parliament and of the Council on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC; see http://ec.europa.eu/health/files/eudralex/vol-1/reg_2014_536/reg_2014_536_en.pdf

Prior to making any data available to a third party, you must enter into a binding legal agreement with that third party, specifying for which purposes they may process the data. This description must be aligned with the information you've provided to the user (i.e. the third party may not be instructed to process the data for purposes that you would not be allowed to do), and the agreement must forbid the third party from processing the data for any other purposes. This is particularly crucial if the third party intends to conduct substantial processing operations. In this case, there is a greater risk that these operations are not compatible with the purposes communicated to the user than with purely technical services. Note that, if the third party processes the data for its own purposes, you are required to assess in advance whether this transfer is legally permissible, notwithstanding the third party's own responsibility for complying with applicable data protection rules itself.

The agreement must contain sufficient security obligations for the third party, which are aligned with the security measures that you have developed yourself (i.e. security may not be weakened by entrusting data to a third party).

When selecting a third party, you must consider any data transfer restrictions under applicable law (see the question below).

Finally, you must ensure that the liability of the third party is sufficiently clear and appropriate to cover potential damage suffered by your users.

Keep in mind that it is your responsibility to select appropriate third party service providers, and that you may be liable towards your users if any incidents with the third party cause them harm.

9) Where can I transfer the gathered data to?

As noted above, the user may store any data on his/her own device. If you have obtained the proper consent, you may also store the data on your own servers (i.e. systems under your sole control, at the exclusion of any third party service provider).

If you wish to transfer data to a third party, you must conclude an agreement that satisfies the requirements as explained under question 5 above. Furthermore, you must consider the physical locations where the data will be transferred, as EU data protection law has restrictions on transferring data to locations outside the EU/EEA[24].

If you wish to transfer data to a location outside the EU/EEA, you must ensure that you have legal guarantees that the transfer is permitted under European law. To do so, one or more of the following conditions must be satisfied:

[24] The European Economic Area (EEA) consists of the EU and Iceland, Liechtenstein and Norway.

- The locations are countries which are covered by an adequacy decision of the European Commission[25].
- The third party has provided appropriate contractual guarantees through the European Commission's Model Contracts for the transfer of personal data to third countries[26], or through the conclusion of Binding Corporate Rules (BCRs)[27].
- Transfers are also permissible if you have obtained the user's unambiguous consent to the proposed transfer. However, consent is only a valid ground for occasional and clearly identified transfers, not for repeated or structural transfers[28]. If the app frequently and systematically transfers data to a location outside the EU/EEA, one of the two aforementioned conditions should be satisfied.

10) What shall I do if there is a personal data breach?

A data breach occurs when personal data is subjected to an incident leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, that personal data. This could seriously affect your users' confidence in your app, so be aware and prepared.

The following questions may be helpful as a checklist to go through as you build your app, and if you think that there has been a data breach. You should review this list and prepare a response to breaches *before* a breach occurs:

1. You should evaluate whether the breached data is considered to be personal data.

   E.g. does the breached data contain name, address, email address, phone number, credit card or other payment information, data concerning health related to an identifiable individual, IP address where it is held with other data from which the individual may be identified? If no, then this event may not be a data breach relating to personal information and no further action may be necessary. If yes, then proceed to the next step.

2. You should check whether there is an obligation to notify a Data Protection Authority (DPA) in a specific country or countries. This may be determined by your place of establishment in the EU or, if you are not established in the EU, the location of your local representative. If in doubt

[25] For an overview of countries with adequacy decisions, see http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm.
[26] For an overview of permitted contracts, see http://ec.europa.eu/justice/data-protection/document/international-transfers/transfer/index_en.htm
[27] For an overview of BCRs, see http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/index_en.htm
[28] For more information on this interpretation, see the Article 29 Working Party Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995; see http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2005/wp114_en.pdf, p.11

you should contact a competent data protection authority[29]. As of 25 May 2018, data breach notifications to DPAs will generally be mandatory across the EU under the terms of the General Data Protection Regulation.

3. You should check whether there is a specific timeline specified in which to make such a notification. As of 25 May 2018, data breach notifications to DPAs will need to be made without undue delay and, where feasible, not later than 72 hours after having become aware of the breach across the EU under the terms of the General Data Protection Regulation.

4. You should check if there are specific requirements for making such notification, including the information that must be included in them. As of 25 May 2018, data breach notifications in the EU will need to at least:

> (a) describe the nature of the personal data breach including where possible, the categories and approximate number of persons concerned and the categories and approximate number of personal data records concerned;
> (b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
> (c) describe the likely consequences of the personal data breach;
> (d) describe the measures taken or proposed to be taken by you to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

5. You should check whether there is an obligation to notify affected individuals. As of 25 May 2018, data breach notifications to affected individuals will generally need to be made without undue delay across the EU under the terms of the General Data Protection Regulation, unless:

> (a) you have implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;
> (b) you have taken subsequent measures which ensure that the high risk to the rights and freedoms of app users is no longer likely to materialise;
> (c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

If a notification to affected individuals is necessary, you should at least:

> (a) describe in clear and plain language the nature of the personal data breach;
> (b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
> (c) describe the likely consequences of the personal data breach;

[29] For a list of European data protection authorities, see http://ec.europa.eu/justice/data-protection/bodies/authorities/index_en.htm

(d) describe the measures taken or proposed to be taken by you to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

6. You should check what caused the breach, and address the problem as soon as possible to avoid further breaches.

11) How shall I treat any data gathered from children?

With regard to apps which, because of their design or functionality, are particularly aimed at children under the age of 16 or which are particularly likely to be used by such children, you must pay attention to the age limit defining children or minors in national legislation, choose the most restrictive data processing approach in full respect of the principles of data minimization and purpose limitation, and refrain wherever possible from collecting data through children in relation to their relatives and/or friends.

Parental involvement is crucial for such apps. Therefore, you must undertake reasonable efforts to verify that consent is given or authorised by the holder of parental responsibility for the processing of health data of minors.

III. Annex I - Privacy Impact Assessment

This Privacy Impact Assessment (PIA) is intended to help you, as the app developer, to determine whether you've respected the main requirements of the Code, and whether you've followed good privacy practices before making the app available.

The PIA is not legal advice, and cannot provide you with perfect assurance that your app operates in compliance with data protection law. It does not affect your obligations under data protection law, which you will still need to fully adhere to. Specific legislation may require you to use other templates, and using the present document may not be sufficient to meet this requirement.

The PIA has been written to ensure that it can be completed by anyone with sufficient knowledge of how the app was created and how it operates. It does not require specific legal or technical expertise.

When using the PIA, please answer all of the following questions truthfully and accurately. If you don't know the answer to a specific question, or if you don't understand the data protection relevance of a question, you may wish to seek external advice.

Question 1: Which kinds of personal data will be processed by your app? Please explain briefly why this data is necessary to achieve the functionality of your app.

Your answer:

Question 2: For which purposes will this data be processed? This includes the functionality of your app, but also technical processes (e.g. backups), further processing (e.g. big data analysis) and monetisation.

Your answer:

Question 3: How have you obtained the consent of your users to process their data for every type of use foreseen? Have you ensured that you used accessible language? Finally, is the app

particularly likely to be used by minors, and if so, have you implemented processes to involve the parents or guardians?

Your answer:

Question 4: Did you designate anyone to answer privacy related questions in relation to your app? And have you informed the users clearly on how they can contact that person?

Your answer:

Question 5: Was the app developed in consultation with a health care professional to ensure that the data is relevant for the purposes of your app and that it is not misrepresented to the users?

Your answer:

Question 6: Explain what you've done to respect the following security objectives, or explain why they are not relevant to your app:

Objective: app has been developed in accordance with the principles of privacy by design and privacy by default ***- data has been pseudonymised or anonymised wherever possible*** ***- appropriate authorisation mechanisms have been built into the app to avoid unlawful access*** ***- effective encryption has been used to mitigate the risk of breaches*** ***- the need for independent system security audits has been considered*** ***- the app informs users when an updated version is available, and blocks all uses of old apps if the update is security critical*** *Your answer:*

Objective: app has been developed using known guidelines on secure app development and/or secure software development
Your answer:

Objective: app has been tested using mock data prior to making it available to real end users
Your answer:

Objective: incidents that affect remotely stored data can be identified and addressed
Your answer:

Question 7: If any personal data collected or processed via the app is transferred to a third party, then you've obtained appropriate contractual guarantees with respect to their obligations (including notably the purpose limitation, security measures, and their liability). These guarantees take into account whether the data will be transferred outside of the EU/EEA, if applicable.

Your answer:

IV. Annex II – Information notice and privacy policy

As already indicated above, the sample text provided below is only a guideline that may help you get started. It is not advisable to simply copy the text into your app; you must review carefully which changes are needed to ensure they apply to your app, and make the necessary updates.

Example of a condensed notice

This app is made available to you by the mHealth App Company (www.mhealthco.eu). The app allows you to register and monitor your blood pressure values. If you choose to, we will create backups of your data. We will not sell your data to third parties, or make it available to them for other purposes than to enable your use of the app.

You can access, correct and delete your data at any time via the app itself. For any questions regarding your data or privacy protection, please contact us via privacy@mhealthco.eu. For more detailed information, click here.

If you accept the above, click the 'I agree' button below to continue.

Example of a full privacy policy – available to the user if she clicks on 'click here' in the condensed notice, or at any time thereafter via a privacy button in the app

This app is made available to you by the mHealth App Company (www.mhealthco.eu), a company under Belgian law, established at Fictitious Road 1, 1000 Brussels, Belgium. The app allows you to register and monitor your blood pressure values.

If you choose to, we will create backups of your personal data. In this case, mHealth App Company will act as the controller under applicable data protection law. If you choose to retain personal data only on your device, it will remain under your own sole control and responsibility at all times.

The personal data processed via this app consists of:

- Any identification data entered by you, the user, specifically your username, age, and nationality;
- Your contact information, specifically your e-mail address and phone number;
- Device identifiers and technical information pertaining to your device, your user account on the device, and your use of the app on this device;
- Data concerning health as entered by you, specifically your blood pressure values, weight and height.

If you allow mHealth App Company to store your data:

- Your data will only be used for back-up purposes, allowing you to restore the data to any compatible devices you own and to synchronise the data between these devices;
- Your data will not be sold to third parties; nor will we allow third parties to use your data for their own purposes. However, backup services may be outsourced by mHealth App Company to a third party service provider. mHealth will ensure at all times that the third party service provider will be bound by an appropriate agreement in accordance with applicable data protection law, and ensuring at all times that your data will remain protected in accordance with at least the same standards as under the present privacy policy.
- You can access, correct and delete your data at any time via the app itself. For any questions regarding your data or privacy protection, please contact us via privacy@mhealthco.eu.
- mHealth App Company will implement appropriate technical and organisational measures and procedures in such a way that ensures the protection of your rights, and always in accordance with applicable data protection law.
- In case of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, your personal data, mHealth App Company will inform you of the breach without undue delay, including a summary description of the potential impact and a recommendation on measures to mitigate the possible adverse effects of the breach.

You may at all times cease to use the app and/or uninstall it. If you uninstall the app, you will be given the choice whether you also wish us to delete any data that you've asked us to back up. If you do not use the app for more than a year, mHealth App Company will automatically delete any data you've backed up.