Draft Code of Conduct on privacy for mobile health applications

I. About this Code

1) Introduction

To be drafted as a last step, when the rest of the Code is more or less stable – Ed.

2) Purpose

The purpose of this Code of Conduct (hereafter the 'Code') is to foster justified trust among users of mobile applications (hereafter 'mHealth applications' or 'mHealth apps') which process personal data that includes data concerning health. More specifically, users of such mHealth apps should be able to assess more easily that any processing of data concerning health via these apps is done in a fair, lawful and transparent manner, in accordance with applicable data protection legislation, and that it provides a high level of security. 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 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, "data concerning health" should be understood as any data related to the physical or mental health of an individual, or to the provision of health services to the individual. Data concerning health[3] in particular includes any data that describes the health status or health risk of an individual or that describes medical interventions undertaken by the user.

---

[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.

[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-

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 or heartbeat rhythm solely as a way of measuring the users' sports activities. **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 to enable medical follow-up** (e.g. by automatically notifying emergency services when required), **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 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 is subject to more stringent legal requirements.

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.

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

29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_annex_en.pdf

[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

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.

4) Adherence to the Code & governance

To be discussed with a broader constituency and finalised thereafter. The Governance – Adherence section should at any rate ensure:

- *That accessibility to SMEs is clear; this implies either no cost or a very minimal cost;*
- *That enforcement is somehow enabled. That does not necessarily require a governing body that can make adjudication decisions, but we need to be able to show how we support enforcement.*
- *That maintenance and revision of the Code are possible.*

A simplified structure in which the necessity for a central body is avoided as far as possible could rely on the following principles:

- *The Code relies on self-assessment and self-declarations of compliance, so that no external audits/certifications are necessary (thus minimising costs);*
- *App developers need to publish a statement of compliance themselves, possibly including the PIA to facilitate verifications and enforcements;*
- *Maintenance and revision are addressed in the same manner as the current drafting process: the European Commission acts as a convener towards the industry, and industry members update the Code as required.*
- *Enforcement remains a responsibility of national DPAs, assisted of course by any publications/statements provided by the app developers (which support accountability by requiring them to actively assess and communicate how they believe to be complying with data protection law)*

The main complexity is adherence. If the Code relies on mere publication by the app developers of declarations of compliance – without external verification or publication - then a greater burden and risk is placed on the end users. Such declarations could typically be enforced in practice, since false

declarations or declarations that the app developer does not adhere to will typically be contrary to data protection law and/or be considered an unfair market practice. However, in both cases the end user would need to take enforcement action and would need to be able to prove that a certain statement was made at a certain point in time. A central or at least federated register would reduce this risk if it publishes and retains a list of app developers and their declarations, so that app developers could not trivially remove or edit their declarations.

Options for such a model include:

- *Publication by a governmental body. Options would include the Article 29 Working Party (or the future European Data Protection Board), or the EDPS. While this is not how current Codes operate, it may be a viable option in view of the political goal to support future Codes of Conduct (i.e. other Codes may benefit from a similar register). It has the benefit of allowing adherence to the Code to be free of charge for the developers.*
- *Publication by a network of governmental bodies such as the national DPAs publishing notices originating from their respective jurisdictions. This has the same advantages.*
- *Both of the options above would have the drawback of incorrect perception: public bodies may not wish to appear to be involved in the governance of an industry Code. The alternative is for a private sector body to manage the register. Presumably this would involve a publication fee to cover operating costs, thus removing the benefit of the zero-cost model. The perception would also be different, since the initiative is less likely to be seen as authoritative, even with a beneficial opinion from the Working Party. This will make marketing/promotion more challenging.*

Initial feedback from stakeholders took the following form:

- *One stakeholder (an mHealth app developer) stated that the Code needed a clear business model with a recognized certification process in order to be useful and to inspire trust. It suggested the creation of a central body with a budget that would be adequate for sustainability and independence, outside of direct governmental involvement. A tiered contribution structure was suggested where adhering app developers pay for certification by the central body with fees dependent on turnover. For small developers, they would be permitted to self-certify, paying a reasonable flat fee for the publication of their declaration. To avoid capture by dominant players, a strong constitution document would be needed, with a Board of trusted figures.*
- *A second stakeholder (a national trade association) stressed that strong governance would be needed to meet the minimum requirements set out by the EU-Principles for Better Self- and Co-Regulation, with clear mechanisms for consistent monitoring and dispute resolution. The Code should not rely on DPAs for enforcement; the current draft General Data Protection Regulation attributes this role to private bodies or SROs accredited by supervisory authorities.*

Further feedback is desirable to confirm the trend, but provisionally there appears to be an interest for stronger governance with a central body certifying compliance, if affordability can be adequately ensured, especially for SMEs.

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.

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

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.

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

<u>Purpose limitation</u>

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 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.

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.

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?) will provide further guidance on the information you should give.

Privacy by design and privacy by default

Privacy by design[5] 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.

Privacy by default[6] means that, wherever the user has a choice with respect to the processing of his or her data, by default the least privacy invasive and compliant choice is made.

[5] 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*."

[6] 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.*"

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[7], and respect these at all times.

It is advisable to implement user friendly interfaces in your app that facilitate the exercise of these 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 delete their data. 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 much details. For this reason, a layered approach is recommended where users first receive a condensed notice in which they receive the most crucial information,

[77] 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.

and have the possibility of clicking through to a full privacy policy in which all other relevant elements are contained[8].

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;
- 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; **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. Clear criteria must be set for the deletion of data, and these must be clearly communicated to the user, along with the consequences.

[8] 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

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.

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.

In order to secure personal data processing, app developers must assess the personal data processing activities within their app, identify possible data protection risks, and take appropriate mitigating measures. They 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.

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[9] and secure software development[10]. 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[11] and privacy by default (i.e. wherever the user has a choice with respect to the processing of his or her data, by default the least privacy invasive choice is made);

[9] 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

[10] 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

[11] 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-

- E.g. you should consider if data can be pseudonymised or anonymised without impairing the app's functionality;
- E.g. you should consider whether you can build appropriate authorisation mechanisms into the app to avoid 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[12] under the following conditions:

- The use of advertisements must be clearly communicated to the user before any data processing takes place.
- If the advertisement is shown within the app by the app developer or by a third party that doesn't receive any personal data relating to the app user, and the advertisement is strictly related to the functionality and context of the app without requiring any 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.

---

design and the GSMA Privacy Design Guidelines for Mobile Application Development at http://www.gsma.com/publicpolicy/privacy-design-guidelines-for-mobile-application-development

[12] It should be noted of course 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.

- If these conditions are not met (i.e. because the advertising is provided by a third party such as an ad network that receives the app user's personal data, or because it involves the creation of user profiles across multiple apps and services, or because the advertisements are not restricted to the functionality or context of the app, or because data concerning health is processed to target the advertisements), then the prior opt-in consent of the user must be obtained[13]. 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.

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 historical, statistical or scientific 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 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 laws apply, and respect any restrictions. Typically this implies that you will need to anonymise data wherever possible, or pseudonymise it[14]. 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[15], 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. 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) is subject to normal data

[13] 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

[14] 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

[15] 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

protection rules, and will thus usually require you to ask for new 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.

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.

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[16].

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:

- The locations are countries which are covered by an adequacy decision of the European Commission[17].
- You have obtained the user's unambiguous consent to the proposed transfer;
- The third party has provided appropriate contractual guarantees through the European Commission's Model Contracts for the transfer of personal data to third countries[18], or through the conclusion of Binding Corporate Rules (BCRs)[19].

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

A data breach occurs when personal data is subjected to an incident resulting in 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

[16] The European Economic Area (EEA) consists of the EU and Iceland, Liechtenstein and Norway.
[17] For an overview of countries with adequacy decisions, see http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm.
[18] For an overview of permitted contracts, see http://ec.europa.eu/justice/data-protection/document/international-transfers/transfer/index_en.htm
[19] For an overview of BCRs, see http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/index_en.htm

EU or, if you are not established in the EU, the location of your local representative. If in doubt you should contact a competent data protection authority[20].

3. You should check whether there is a specific timeline specified in which to make such a notification.

4. You should check if there are specific requirements for making such notification, including the information that must be included in them.

5. You should check whether there is an obligation to notify affected individuals. Does this obligation arise from advice or guidance provided by the DPA at the previous step or separately? Are there specific requirements in relation to what information must be provided to the affected individuals?

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 or which are particularly likely to be used by 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 implement a process to obtain appropriate parental consent for the processing of health data of minors as required under applicable law.

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

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 notices

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, this data will be backed up on our own servers. Your data will never be sold or otherwise shared with third parties.

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, this personal data will be backed up on our servers. 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 never be sold or otherwise shared with third parties. 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 the 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 backed up to our servers. If you do not use the app for more than a year, mHealth App Company will automatically delete any data you've backed up to our servers.