Brussels, 10 April 2017

Hans Graux
Project editor of the draft Code of Conduct on privacy for mobile health applications

By e-mail: hans.graux@timelex.eu

Dear Mr Graux,

The objective of the Article 29 Working Party (hereafter "WP29") is that the application of the code ensures that individuals feel confident that their data are used appropriately. In that respect, WP29 welcomes the open and constructive dialogue with industry representatives and other actors in the health sector as part of the review of the proposed Code of Conduct.

First of all, I would like to underline that a code of conduct needs to be compliant with the Data Protection Directive and with the national provisions adopted pursuant to the Directive. Furthermore, the code of conduct must be of adequate quality and must provide sufficient added value to the Directive and other applicable data protection legislation. Added value can be demonstrated, for example, by addressing specific data protection questions and problems encountered by organisations or within the sector to which the Code is intended to apply by offering effective and clear solutions for these questions and problems. This has already been established by the WP29 in the Working Document WP13 on the procedure for the consideration of Community codes of conduct[1].

I would also like to point out that pursuant to article 40.2 of the General Data Protection Regulation (hereafter the "GDPR"), the purpose of drafting a code of conduct is to specify the application of the Regulation. Therefore to ensure the continued relevance of the Code post transition to the GDPR, it is important that you take this requirement into account at this stage.

The WP29 has analysed the Code of Conduct's compliance with the Data Protection Directive and in light of the GDPR requirements. We stress however that compliance with national legislation adopted pursuant to the Directive will be assessed in full at a later stage.

General comments

While the Code is intended to provide a framework for developers to adhere to that should create a transparent and trusted app development environment, WP29 is of the opinion that the current provisions in the Code do not bring sufficient added value to the Directive and

[1] DG XV D/5004/98, WP 13, Future work on codes of conduct: Working document on the procedure for the consideration by the Working Party of Community codes of conduct, adopted on 10 September 1998

provisions made in national law. The Code would benefit from further clarification in some areas as well as references to the existing legal framework. WP29 has provided examples below which we believe will help strengthen the Code. These examples are not exhaustive and for sufficient added value more sector specific explanation of the applicable legal framework needs to be incorporated into the Code. When revising the Code, we would therefore encourage you to consult with your stakeholders to identify other areas in which the code can be improved.

Firstly, the Code does not elaborate sufficiently on the relationship between the data protection directive and the national legislation implementing the directive in the individual EU Member States. In particular, in the section headed "How should I obtain the consent of the users of my app?" the Code refers to the processing of data for research purposes. This is an area where, under Article 89(2) of the GDPR, Member States will have discretion to adopt national rules on processing.

Secondly while we note that the Code "aims to facilitate data protection compliance" and does not address "other compliance issues", we strongly recommend that it takes into account other legislation which impacts on the prime objective of data protection compliance. For instance, there are elements, notably cookies, in the ePrivacy Directive which ought to be considered. We acknowledge however that to fully consider the implications of this directive is a challenge at the moment because it is currently being revised. Furthermore, you need to consider issues raised by other legislation such as banned practices under the Unfair Commercial Practices Directive or as part of the EIDAS regulation or the Council Directive 93/42/EEC concerning medical devices.

Thirdly, the Code needs to be clearer on the roles of the parties involved in processing. App developers could assume a role either as data controller or data processor, or possibly both depending on the circumstances. The differing roles carry with them a different level of obligations. Additionally, when addressing the issue of disclosing data to third parties, the different responsibilities of the parties also need to be clarified depending on the developer's role (i.e. as a processor, co-controller or separate controller).

Health data

With regards to the section on health data and lifestyle data, the Code needs to be re-evaluated in light of the relevant provisions of the GDPR (art 4.1 and recital 35) as well as the text of the Annex to the letter of 5th of February, 2015[2] to ensure that the content of the Code is consistent with the definitions given in the Data Protection Directive and the GDPR.

In particular, you should consider the threshold specified in the Code, that for lifestyle data to constitute health data it needs to be "inherently related to" an individual's health, or that there's a "clear and close link" to a person's health status, and whether this is different to the threshold specified in the Data Protection Directive and the GDPR.

Specific comments

In addition to the above general comments, the WP29 has further observations and questions on specific areas of the code, which, in its opinion, need to be addressed in order to improve the quality, value and application of the Code.

[2] 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

Governance and monitoring model

WP29 was unable to ascertain whether the governance model as detailed in the Code will be compliant with some of the new requirements of the GDPR, in particular articles 40.4 and 41.2.

With reference to article 40.4, WP29 recommends that further detail is added to explain how the governance bodies will monitor the controllers and processors committed to apply the Code. In particular, the Code should clearly define concrete sanctions and remedies as well as the dispute resolution mechanisms needed as part of a credible governance and enforcement model. Similarly, there is scope to increase information transparency by, for instance, making information publicly available about breaches of the Code and clarifying how national Data Protection Authorities will be informed about breaches of the Code. It would also be helpful to provide further information about the criteria for the periodic monitoring, including timing, the minimum number of apps that will be formally reviewed by the monitoring body and the methodology used to assess those apps.

With regard to article 41.2, the Code needs to clarify how the different governance bodies identified will maintain their independence, impartiality and transparency. The Code also needs to clarify how panel members will be selected and their independence ensured (for example there is no further information as to the qualifications and eligibility conditions required to be appointed as member of the panel, etc.).

Furthermore, WP29 is of the opinion that the Code must be more specific on the composition of the Assembly and how the membership is managed. This should include details of how end users and the data protection community are represented. This is required to ensure (as indicated in the Code) that it is "driven by associations and other bodies involved in the mHealth ecosystem" and that "all relevant voices can be heard".

With reference to the monitoring body specifically, certain information will be required to demonstrate that this body can be accredited pursuant to article 41.2 of the GDPR. By no way exhaustive, the information provided in the code should include the sector affiliation and the number of the representatives by sectors. It should also include information about the independence of representatives, their expertise in relation to the subject matter of the Code and the absence of a conflict of interests. Information should also be provided about the procedures established for the monitoring body to carry out its functions, for example, with regard to the number of apps reviewed and any actions to be taken as a result of those reviews.

Additionally, further information is needed about the financial contributions required from the different actors/members. Without this information there is a concern that the level of fees may prevent the participation of a wide range of end user representatives, and, hence, create an imbalance of interests among the members of the General Assembly.

WP29 welcomes the fact that the Code introduces the notion of third-party certification to complement self-declared compliance. It however recommends that the Code makes the benefits of certification, as well as the mechanisms governing it (re: information transparency and monitoring), clearer to the audience; the more so given that the costs associated with certification and third party audit will be borne by the app developers. WP29 is aware that further guidance on how certification will work under the GDPR is necessary and it is currently working on such guidance. In any case, the Code should make clear that the certified app developer should turn to the appointed Data Protection Authority whenever required by data protection rules such as in case of data breaches.

Finally, for avoidance of any doubt, WP29 wishes to point out that it, or its members, will not be a member of the Assembly or in any other way participate in the governance or monitoring mechanisms of the Code.

Practical guidelines for data controllers

This section of the Code implies that the processing of personal data in most mHealth apps is almost exclusively based or dependent on the consent of individuals. WP29 is concerned that consent might not always be freely given by individuals, particularly if the use of the app has been recommended to them. Therefore, the Code should make clear, that the consent should fulfil all requirements of the GDPR and the Data Protection Directive regarding consent. Additionally, the WP29 recommends that the Code acknowledges that there are other conditions, besides consent, which render the data processing fair and lawful and that, therefore, the Code makes more *explicit* reference to these other conditions. Similarly, the section on consent should also make the point about *issues* relating to *the processing of data held by third parties, general data retention rules and* practical *aspects of consent withdrawal*. For example, the Code needs to be clearer on which requirements third parties need to meet when consent is withdrawn; this includes clarifying what happens to the personal data processed by third parties when the data subject withdraws his or her consent.

In relation to processing of children's data, WP29 considers that the guidance provided by the Code in relation to a guardian's consent verification should be addressed more thoroughly. In particular, the code should consider different possible situations in which apps can demonstrate how consent has been given by the guardian.

WP29 would also encourage the Code to identify suitable safeguards to raise data subjects' awareness of the possible risks associated with the use of mHealth apps. This is particularly important where the app for likely to be used for processing sensitive personal data or children's data. In general adequate safeguards should be provided when children's personal data are processed (see the WP202 on apps on smart devices and the special attention reserved to children by the GDPR).

Data protection principles

Regarding the "practical guidelines for app developers" which are at the core of the Code, WP29 recognises that many data protection principles have been embedded in the document. Particularly relevant in that respect are references to the purpose limitation and compatibility of secondary uses of health data and the necessity of safeguards for data subjects (i.e. increased transparency, including a clear possibility to object, and the use of encryption or pseudonymisation techniques). Regrettably, the Code does not mention the fact that these safeguards should also be "appropriate".

WP29 notes that the Code does not refer to other relevant principles of the processing of personal data, such as the accuracy and quality of data, its accessibility and security issues linked with data storage. The code should either include reference to these other principles or explain why they are not seen as relevant. Further, certain data protection principles, while touched upon, would merit more context as well as concrete examples of situations where the processing of data would call for specific attention to those principles. For instance, it is unclear from the Code that the principles of accountability (Article 5.2 of the GDPR: the controller shall be responsible for, and able to demonstrate compliance) and data security are

legal requirements which app developers must comply with, as opposed to good practice elements which they should have regard to.

Information, transparency and data subjects rights

As mentioned above, WP29 is of the opinion that the terms of 'data controllers' and 'data processors' should be brought up to clarify the roles and exact responsibilities of the app developers in relation to the requirements of the Data Protection Directive (and the GDPR) as well as of the implementing national legislation. At the very least, we would expect that, where the developer has a role as a data controller, relevant information about the data controller (i.e. identity and contact details; in case of co-controllership, a single point of contact should be offered to the user) would be available to the end user[3] and that this information should be provided to the data subject prior to the start of the data processing. This is clearly specified as a requirement in the GDPR. In this context, the WP29 notes that for example, it would often not be sufficient to inform the user if personal data is made available to a third party for processing operations. Instead, an informed opt-in consent, or other legal grounds, would be necessary.

We note that the Code offers examples of privacy notice generators. We urge you to review the references provided in the text: (a) the Intuit Mobile Privacy Notice Code covers only two categories of information: (1) the type of data collected by the app and the purpose of processing and (2) the types of third party companies with which data are shared with; (b) the sign-in function for the MEF Mobile Policy Generator no longer works, and makes the Generator unusable.

The Code does not provide sufficient information or practical examples on how data subjects can exert their rights and on how controllers and processors ought to meet their obligations related to data subject rights. Furthermore, the future right to data portability (as enshrined in the GDPR) needs to be elaborated upon insofar as it may bear significance to the processing covered by the Code. For your information, WP29 published draft guidelines on data portability on 13 December 2016. The draft has been open for consultation and a revised version can be expected later this year. It is also recommended that the Code elaborates on the right to erasure in accordance with Article 17 of the GDPR.

Finally, WP29 would also welcome more detailed guidance on how app developers should approach upgrades and the requirement to notify users in case the upgrade changes the scope or nature of the processing.

Security

The Code should include more details and relevant examples on how app developers can integrate "privacy by design" and "privacy by default" in their development process as well as be attentive to legal restrictions relating to retention periods. It should be noted that these two requirements are not merely related to security. Privacy by design is a basic requirement of the GDPR with regard to any processing operation, and security measures are part of the privacy design approach.

With reference to the anonymisation of the data for research purposes, WP 29 welcomes the Code's reference to its Opinion 05/2014 on Anonymisation Techniques, adopted on April 10th 2014, as well as the correct assessment that data controllers must notify users of the further

[3] According to Article 10 of the Data Protection Directive and according to Article 13.1.a of the GDPR

processing. WP29 would however recommend that the Code is more explicit as to what a "completely anonymized dataset" entails. As you will know, the WP29 Opinion meant that, for anonymisation to be in effect, the data must be processed in such a way that it can no longer be used to identify a natural person and that this processing is "irreversible". We would therefore encourage the Code to raise awareness among app developers and data controllers of the risk of re-identification.

WP29 welcomes that the Code usefully recommends effective encryption of data processed, but would advise that it also addresses the issue of secure transmission, as this not only implies encryption but also strong authentication. In this regard, WP29 would like to point out that the Code does not adequately consider the cases where the users would like to allow third parties (e.g. their personal doctors) to have access to their data; such cases raise several security issues, such as the necessity of a strong authentication mechanism to ensure that only relevant third parties (e.g. doctor) has access to the data, as well as that the type of access is exactly the one for which the user has provided explicit consent.

Marketing

The section on advertisements should be strengthened to clarify the legal basis and requirements for processing data for marketing purposes and could refer to Recital 47 and Articles 6 and 7 of the GDPR.

Reiterating a point mentioned earlier in this letter, the issue of consent, and explicit consent in connection with the processing of sensitive data, is a key element to ensure that the further processing is fair and lawful. The Code should provide guidance on how this can be expressed by the data subject.

WP29 would like to draw particular attention to the following statement: "it is permissible for the app to make acceptance of advertisements a condition of the use of the app". You will note that under Article 7(4) of the GDPR, consent cannot be considered to be freely given if the performance of a contract/provision of a service is conditional on consent to the processing of personal data not necessary for the performance of that contract/provision of that service. In other words, a controller may not make a service conditional upon consent, unless the processing is necessary for the service, which WP29 would dispute, might not be the case regarding behavioural advertising. We would therefore ask that you reconsider this statement.

Transfers to third countries

A reference to art. 48 of the GDPR may be added in order to address the issue related to transfers of personal data to public authorities and commercial entities based in third countries. The Code should in any case require that information on where data will be transferred is provided.

Personal Data Breaches

Lastly, when assessing whether the breached data is considered to be personal data, the definitions of the 95/46/EC Directive and the GDPR should be taken into consideration (in this regard, the example seems to be misleading).

Conclusion

The above points encapsulate WP29's general and specific comments on the submitted draft Code. Please consider these at the earliest opportunity.

When revising the draft, please consider carefully what "added value" the code of conduct provides as a whole and, in particular, what specific examples, practical solutions or recommendations you could draw from discussions with stakeholders, to demonstrate why your Code would merit being approved by the WP29.

While my letter makes various recommendations to amend the text of the Code, I would reiterate that this process should be seen as a dialogue. As such, the *e-government subgroup* of the WP 29, which has led the review of the draft code, is available to discuss the points set out in this letter and would welcome an opportunity to hear more about the practical and technical background as well as the objective of the Code.

Yours sincerely,

On behalf of the Article 29 Working Party,

Isabelle FALQUE-PIERROTIN
Chairwoman