THE DUTY TO INFORM AND OTHER ACCOUNTABILITY MEASURES FOR MOBILE DEVICES

I. INTRODUCTION

This technical note is addressed to those entities involved in the development, distribution and operation of apps for mobile devices, especially those which function as data controllers or joint controllers in each area of competence, as well as other any other agents involved in the mobile device apps environment, as, for example app developers and library developers.

In general terms, the Spanish Data Protection Agency has published several guidelines in order to help comply with the obligations acquired with regard to data protection such as the "Guidelines to comply with the duty to inform", the "Decalogue to adapt the GDPR to Internet privacy policy", the "GDPR guidelines for data controllers" and the "Guidelines to prepare contracts between data controllers and data processors". The then-existing Article 29 Working Party also published "Opinion 02/2013 on applications for smart devices". This technical note extends and completes these resources by establishing very specific guidelines for mobile apps, developing certain specific aspects with regard to the duty to inform and other proactive responsibility measures.

These guidelines are obtained from the conclusions of several studies completed in the framework of collaboration between the Technical University of Madrid (UPM) and the AEPD on mobile apps in the scopes of education and wellbeing, as described Annex I.

II. SPECIFIC GUIDELINES FOR MOBILE APPS

With regard to the duty to inform, an analysis of the relevant mobile apps concluded that certain compliance aspects require special care by the data controllers.

1. The information provided to users with regard to processing their personal data must comply with the requirements set forth in articles 13 and 14 of the GDPR, Article 11 of the Organic Act on Data Protection and Guarantees of Digital Rights, especially with regard to information in layer, in the terms stated by the "Guidelines" and the "Decalogue to adapt the GDPR to Internet privacy policy".
2. Said information, structured into a privacy policy, must be available both in the app itself and in the app store. In the same manner, users may consult this privacy policy before installing the application or at any time during use.
3. Access to privacy policies from the app must be easy and user-friendly, and require a limited number of clicks, ideally a maximum of two, as recommended by the 29 WP in their transparency guidelines.
4. The privacy policy must clearly identify the data controller. When the relevant data controller is located outside the EU and the app is available to European users, a representative in the EU must be appointed and identified in the relevant privacy policy.
5. Information on data processing must be complete and consistent both at the app store and in the app itself. Any discrepancy between the information on

data processing provided in the store and in the app is not allowed. This also applies to any app pre-installed in a device at the time of their purchase.

6. The language used to describe privacy policies must be appropriate for the app target user, considering their age and computer literacy as well as the language used; for example, when an app is targeted to Spanish speakers and thus available in Spanish, the privacy policy must also be in Spanish, notwithstanding that may also be in other languages. These aspects are especially relevant for apps designed for underage users.
7. Privacy policies must be detailed and specific with regard to the data processing to be performed. In order to avoid "data collection fatigue", providing general, not app-specific information must be avoided. Privacy policy must not, for example, describe a set or application or their services by the same organization, such as its website.
8. The app's privacy policy provided to users must include the entire intended data processing, including detailed information on which data and processing activities are necessary for the app's basic operation and which are optional, as well as any relevant additional information about the intended data processing activities. Besides, the privacy policy should state the authorisations requested by the application (either directly or through third party libraries) in order to access data and resources, the purposes and processing activities for which such authorisations are issued and their relevant scope (reading, writing...). For example, the privacy policy must report whether the app shall process data only when executed by any user action on the foreground or whether it also needs to access information when being executed in the background. Users may also be provided information regarding the manner in which they may manage the authorisations granted to the app, so that they may decide at any time whether to grant or revoke such authorisations, or the conditions under which such authorisation is granted.
9. When data processing though the app is justified by reason of user consent, such consent must be obtained independently for each processing scope and procedure. Installing and using an app may not be conditioned to obtaining consent for any data processing activity which is not necessary to provide the service defined for such app.
10. Ambiguous or unclear clauses, such as "any data may be collected, disclosed or indefinitely retained" or "your data are collected in order to improve your user experience" must be avoided.
11. Specific information must be provided on data retention terms and the final destination of data once these terms have elapsed.
12. In this sense, specific information must be included on the logic applied to profiling and automated decision-making, or a link to such relevant information, as well as the logic used to personalize ads.
13. The definition of the purposes of processing and their legal bases must be clearly stated and specific, as well as the identification of those personal data which are collected for each of such purposes.
14. It is important to remember to provide users with information on their rights regarding data protection and providing mechanisms and procedures to perform them in an effective manner.

15. When appropriate, the practice of international data transfer must be explicitly and specifically disclosed.

When data controllers outsource app development, start-up or operation to third parties, and such third parties are granted access to personal data, they must ensure to comply with any requirements established for each party in the GDPR. In these cases, consulting the "GDPR Guidelines for Data Controllers" and "Guidelines to prepare contracts between data controllers and data processors" is especially useful.

The following requirements are especially remarkable:

16. Data processing must be governed by a contract or any other legally binding agreement, which establishes the scope, duration, nature, type of personal data processed, categories of involved parties and rights and obligations of the data controller.
17. The relevant contract must specifically state that the data processor shall process the relevant personal data in strict compliance with the documented instructions provided by the data controller; therefore, the data processor must not enter in the app any other personal data treatment unknown to the data processor, such as to those that may be introduced when including in the app third party libraries for advertising purposes, analysis purposes, or others.
18. The relevant contract must state that the data processor must implement all measures stated by the data controller with regard to processing security. These specifically include the best development practices and consider privacy by default and by design from the app design phase.

Particularly, the following practices must be specifically considered:

19. Ensuring granular management to access authorisations regarding protected system resources, pursuant the provisions set forth by the privacy policy. An example of this is granting authorisations exclusively to a specific resource, such as the images folder, instead of granting a general access permit to the device stored contents.
20. Respecting the user's privacy settings regarding, for example, personalised ads, and preventing, when appropriate, access to advertising identifiers.
21. Preventing access to globally unique identifiers together with advertising identifiers, since this would allow to make assignments that leave user protection measures, such as changing their advertising identifier, without effect.
22. Preventing personal data disclosure to advertising and analytics services from the moment that the app is opened, without giving the user any time or opportunity to make any adjustment in or use of the app.
23. Verifying that personal data are not disclosed unknowingly to the data controller, for the reason of being communications starting in third-party libraries used by developers to enhance the app's functionality or its financial performance.
24. Preventing that personal data are assigned to unspecified recipients or any recipients not disclosed in the privacy policy, who act as data controller or co-data controller.
25. Preventing international data transfers not disclosed in the privacy policy.

26. Using advanced methods for communications encryption (e.g.: *certificate-pinning*[1]) is an additional guarantee for user privacy, and its use may be considered depending on the nature of data processing activities.

III. CONCLUSIONS

Transparency in personal data processing by apps for mobile devices is a key aspect for compliance with data protection laws and regulations, that is, for protecting citizens' rights and freedoms.

The AEPD has made available for data controllers two resources to make easier to comply with the GDPR transparency and information requirements: the more general "Guide for compliance with the duty to inform" y and the more Internet-based app-specific "Decalogue to adapt the GDPR to Internet privacy policy".

This technical note develops previous guidelines and is intended to address app environment specific aspects for which it has been detected that special care is needed.

For this purpose, it must be highlighted that any information provided to the user must be stated in a clear, simple language, and in an intelligible, transparent, earnest, accessible manner, appropriate to the recipient or to the app's potential user. For this reason, it must be considered the app's target users to prepare any informative clauses on privacy policy.

Certain sensors and data storage devices of mobile devices are a potential source of personal data which may be accessed by apps or third-party libraries included in applications. The mobile device operative system protects from access to these resources through permits with different protection levels.

Although the device displays a notification requesting the user's authorisation to access such resources, the displayed information very frequently is not enough under the GPDR, or the granular nature of the permit is not correctly identified, since, among other information it must include the purpose of such data processing. The need to access such resources must be properly included in the app privacy policy, so that the user may decide whether they authorise or not the app to access such resources.

Besides, guidelines are developed for data controllers who outsource app development, start-up or operation to third parties, and such third parties, which are granted access to personal data, must ensure to comply with any requirements established for each party in the GDPR. Such guidelines complement the "GDPR Guidelines for Data Controllers" and the "Guidelines to prepare contracts between data controllers and data processors". Data controllers must ensure to comply with all active responsibility requirements included in the GDPR, and at the same time that data are processed by the data controller in strict compliance with their received instructions and with all necessary measures to ensure compliance.

[1]Technique to prevent interception of encrypted communications by means of MITM attacks: Certificate Pinning Symantec

ADDENDUM I: SOURCE AND METHODOLOGY

This technical note has been developed under the privacy and data protection initiatives in the framework of the 2015-2019 Strategic Plan of the Spanish Data Protection Agency. The first one is aimed to personal data processing carried out by apps for mobile devices used in educational environments, specifically at compulsory education levels, while the second one is focused in apps for mobile devices designed for monitoring the users' physical activity, health and wellbeing. These works have been carried out by the Technical University of Madrid, directed and coordinated by this Agency.

The Strategic Axis 2 "Innovation and data protection: trustworthiness and quality assurance" of the 2015-2019 Strategic Plan of the Spanish Data Protection Agency establishes an action line which creates the Unit of Evaluation and Technological Studies, one of whose goals is to prepare studies and reports regarding technological studies and projects (section 2.5 of the aforementioned plan).

In this sense, the Spanish Data Protection Agency addressed the need to carry out a proactive initiative among the managers of products and services in relation to which personal data are processed. Specifically, the need to carry out studies on the so-called connected society, including the works which are the subject of this report, is addressed, since data used in this context are especially sensitive due both to the source subject (which, in the study carried out in compulsory education environments are underage students) and to the nature of data (which, in the study on physical study monitoring, were healthcare-related data).

At the same time, collaboration between this Agency and the academia is to be reinforced in order to promote technical research oriented to improve privacy and data protection.

Such works involved some basic research aimed at:

- Analysing information flows in apps for mobile devices in general.
- Designing standard procedures which allow to carry out application privacy assessments in a systematic, comparable and orderly manner
- Assessment of a representative subset of applications which are useful in the educational, healthcare and wellbeing scopes.
- Assessment of privacy policies with regard to the decalogue for adaptation to the GDPR published by this Agency.

The ultimate purpose is to detect those practices which are most damaging to user privacy, considering both groups of users, for the purposes providing solutions or alternatives for developers, promoters and users of such applications.

This report aims at highlighting the main conclusions obtained from both studies, which may also apply to other mobile apps.

In the framework of those works, a total of 20 apps for Android devices, 10 for each scope of study (education and wellbeing) have been analysed.

The criteria used for selecting applications have been:

- Most downloaded applications in the Google Play Store intended for Spanish speaking user for each scope of study

- Uniform balance between apps developed and published by small developers, but which are hugely popular among users, and apps developed and published by large tech companies.
- Uniform balance between paid apps and free apps.

For those physical activity monitoring apps that work together with an external device (for example, an activity wristband), the app was analysed when connected to the activity wristband.

The methodology for such works includes a technical analysis of information flows for each app using static and dynamic analysis techniques and comparison against an analysis of the privacy policies for each application. Therefore, for each application, a double analysis has been carried out. First, the privacy policies for each app are compared against the decalogue on privacy policies published by this Agency. Subsequently, any discrepancies between the principles stated in the privacy policies and the observations resulting from the static and dynamic analyses are identified.