GUIDELINES FOR SOCIAL DISTANCE AND ACCESS CONTROL APPS DUE TO COVID-19

The implementation of the Plan for the Transition to a new normality of the Ministry of Health and the expected return of tourism poses a challenge for both companies and public administrations in the management of capacity control or social distance in public places. New initiatives based on app mobile applications are designed. This note provides guidelines for the design of processing based on such applications to comply with data protection regulations. The aim is the following: in addition to provide real guarantees for the protection of citizens' health, to avoid a risk to their rights and freedoms. These recommendations are oriented to current purpose but are also valid to guide the design of future processing to fight Covid-19 based on apps.

The AEPD Report "Use of Technologies in the Fight against COVID19" analyzed some apps that were released at the start of the pandemic such as auto-testing and pre-testing, voluntary infection information, contact-tracing and immunity passports. In these guidelines we will give recommendations for processing based on non-health apps, such as apps to book or control of capacity in beaches, natural spaces and other public places.

In order to control the capacity and social distance social, several entities have deployed their own app, chosing for apps that sometimes combine the book of space with other functionalities, such as geolocation, access control with QR code, recording of the user's personal data or social networks functions. Related to the use these apps, the use mobile phone signaling has been notified, such as the recording of data from the wifi or bluetooth signal.

The AEPD considers that, to achieve the aim pursued, and in application of the principle of minimization, the need to carry out the identification of users in the app must be proved. In this context, the AEPD lays down the following non-exhaustive list of recommendations for those controllers who take the decision to implement these kinds of apps:

1. The purpose must be clearly defined and should be limited to the management of social distance measures such as capacity control or distance control.
2. The proposed processing must be effective in relation to the purpose and cannot generate false safety expectations in accordance with the principle of loyalty of the treatment.
3. The implementation of app-based processing should be based on an analysis of necessity and proportionality that assesses the use of the app and the minimum data set necessary to achieve the objectives pursued. In particular, the identity of the user or their tracking, including the use of unique identifiers of any kind or those from the wifi or bluetooth signal, can only be processed if they are strictly necessary for the purpose of the app.
4. Special categories of data, particularly health data, should not be processed, except those strictly necessary to manage spaces reserved for persons with disabilities.

5. The functionalities of the app should be exclusively those necessary for the specific purposes pursued, not mixing functionalities such as fidelity program, advertising or social networks. Personal data should not be processed for any purpose other than that related to the management of social distance measures that justify the implementation of the app.
6. The use of the app must be voluntary, based on the user's consent for the processing of the personal data necessary for each of the functionalities that are pursued. The processing should be based on free, informed and specific consent. The use of an app should not condition access to public spaces. The controller must provide equivalent alternatives to the use of apps.
7. The controller shall ensure compliance with the principles of the GDPR. It includes to fulfill those provisions relating to set up legal contract with third parties (processors) involved in the processing of personal data. The controller must guarantee that the processors implement the right security measures.
8. In the case of public spaces, the controller must be a Public Body that has the competence to rule it and will decide the purposes and means of the processing.
9. The use of third-party tools or resources for the implementation of the app could include the processing of personal data for advertising purposes, analysis of use or others, in particular the processing of unique identifiers and geolocalizzción data involving the monitoring of people. Therefore, the controller must ensure that processing does not occur.
10. The personal data processed should not be stored beyond the time necessary to fulfill the purposes pursued and, in any case, must be deleted when the purpose is over, except for those data that needed to be kept by legal obligation.
11. As far as possible, common solutions should be adopted for access to different public spaces in the same environment (city, province, region), to avoid exposing users to the potential risks of using multiple apps.
12. The processing of personal data of children under 14 years of age by this type of apps must be consented by their parents or guardians.

Finally, it is advisable to follow the recommendations developed by the AEPD to apply the principles of proactive responsibility that can be found in the Innovation and Technology microsite, specifically those for the development of applications on mobile devices:

- Technical Note: The duty to inform and other proactive accountability measures in mobile apps
- Analysis of information flows on Android. Proactive accountability compliance tools