COVID-19: Tracing applications vs. privacy

Contact tracing and warning applications in the fight against COVID-19 must comply with the GDPR and the e-Privacy Directive. They must be implemented under the supervision of the relevant public health authorities and national data protection authorities.

The European Commission has recently issued guidelines for the development of contact tracing and warning applications in the fight against COVID-19, which can have a significant impact in the control of the disease and play an important role as part of containment measures.

Contents. These applications may include: (i) accurate information about the COVID-19 pandemic for users; (ii) self-diagnostic questionnaires and guidance for users (symptom control feature); (iii) alert notification to persons who have been in close contact with an infected person for testing or be isolated (contact tracing and warning features); and/or (iv) a communication forum between patients and physicians, including providing further diagnosis and treatment advice (e-treatment advice).

Applicable regulations and supervision. Given the extremely sensitive nature of the data (in particular health data) and the purpose of the applications, they must comply with the General Data Protection Regulation (GDPR) and the Electronic Privacy Directive. They must also be implemented in close coordination with and under the supervision of the relevant public health authorities and national data protection authorities.

User control and consent. Users must keep full control over personal data and hence they must give their prior consent (complying with GDPR requirements) and separately for each application's features.

In case of use of location data, this data must be stored on the user's device and only be shared with their prior consent; users must be able to exercise their rights under the GDPR and, among others, they have to be entitled to, at any time, withdraw their consent.

Principle of data minimization and data accuracy. Applications must comply with the principle of data minimization and it may be only processed personal data required for the purpose at stake. For example, for the purpose of tracing contacts, the European Commission considers that the processing of location data is not necessary and thus it does not advise its use.

EU rules require that processed personal data are accurate. Therefore, the Commission considers that technologies such as Bluetooth should be used to more accurately assess contact between different users. The data must be stored on the user's device and encrypted and must only be kept for the necessary period, in medical terms, and for the duration of the containment measures.

For the success of these applications, the confidence of citizens and those who feel safe with their use is essential, which must be ensured under strict compliance with EU rules on personal data protection.

Contacts

Cláudia Fernandes Martins
cmartins@macedovitorino.com

Ana Rita Carmo
rcarmo@macedovitorino.com