CONFINDUSTRIA

EMERGENZA CORONAVIRUS

INFO UTILI PER LE IMPRESE

09 aprile 2020

Raccomandazione UE sull'uso di dati di applicazioni mobili

La Commissione europea ha pubblicato una Raccomandazione contenente una serie di **misure e azioni volte a sviluppare un approccio comune nell'uso di dati di applicazioni mobili in risposta alla pandemia Coronavirus**.
La Raccomandazione definisce un percorso per l'adozione, insieme agli Stati membri, di un pacchetto di misure incentrato su due aspetti:

- un approccio coordinato e paneuropeo per l'utilizzo delle applicazioni mobili al fine di tracciare e allertare gli utenti e consentire ai cittadini di adottare misure di distanziamento sociale efficaci e più mirate;

- un approccio comune per il monitoraggio dell'evoluzione del virus mediante dati di geolocalizzazione aggregati e anonimizzati, al fine di fornire anche utili indicazioni per l'elaborazione di prossime strategie per la riapertura.

Come auspicato da Confindustria e veicolato tramite lo statement redatto in seno alla **Digital Task Force di BusinessEurope**, la Commissione emanerà orientamenti anche in materia di protezione dei dati e di tutela della vita privata in stretto coordinamento con l'European Data Protection Board (EDPB). La Commissione europea invita inoltre gli Stati membri a intraprendere queste azioni con urgenza e in stretta collaborazione con altri Stati membri, la Commissione e tutte le parti interessate.

La Raccomandazione definisce infine i principi fondamentali per l'uso di tali dati nel rispetto dei diritti fondamentali dell'UE, quali la tutela della vita privata e la protezione dei dati. Definisce inoltre:

A. misure volte a evitare il proliferare di applicazioni non compatibili con il diritto dell'Unione;
B. a sostenere la necessità di interoperabilità e a promuovere soluzioni comuni;
C. meccanismi di governance da applicare da parte delle autorità sanitarie pubbliche e in cooperazione con il Centro europeo per la prevenzione e il controllo delle malattie (ECDC);
D. la condivisione di buone pratiche per lo scambio di informazioni sul funzionamento delle applicazioni;
E. la condivisione dei dati con i pertinenti organismi epidemiologici pubblici, compresa la condivisione dei dati aggregati con l'ECDC.

Quanto alle prossime tappe, **entro il 15 aprile gli Stati membri, insieme alla Commissione e in collaborazione con il Comitato europeo per la protezione dei dati (EDPB), elaboreranno un pacchetto di strumenti per un approccio paneuropeo per le applicazioni mobili.**

Gli Stati membri dovrebbero riferire in merito alle misure intraprese **entro il 31 maggio** e renderle accessibili agli altri Stati membri e alla Commissione per una valutazione. La Commissione valuterà i progressi compiuti e pubblicherà relazioni periodiche a partire dal giugno 2020 e per tutta la durata della crisi, raccomandando azioni e/o provvedendo all'eliminazione graduale delle misure non più necessarie.

CORONAVIRUS HOMEPAGE

EUROPEAN
COMMISSION

Brussels, 8.4.2020
C(2020) 2296 final

COMMISSION RECOMMENDATION

of 8.4.2020

on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data

COMMISSION RECOMMENDATION

of 8.4.2020

on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 292 thereof,

Whereas:

(1) The public health crisis caused by the current COVID-19 pandemic (hereinafter, 'COVID-19 crisis') is compelling the Union and the Member States to face an unprecedented challenge to its health care systems, way of life, economic stability and values. No single Member State can succeed alone in combating the COVID-19 crisis. An exceptional crisis of such magnitude requires determined action of all Member States and EU institutions and bodies working together in a genuine spirit of solidarity.

(2) Digital technologies and data have a valuable role to play in combating the COVID-19 crisis, given that many people in Europe are connected to the internet via mobile devices. Those technologies and data can offer an important tool for informing the public and helping relevant public authorities in their efforts to contain the spread of the virus or allowing healthcare organisations to exchange health data. However, a fragmented and uncoordinated approach risks hampering the effectiveness of measures aimed at combating the COVID-19 crisis, whilst also causing serious harm to the single market and to fundamental rights and freedoms.

(3) It is therefore necessary to develop a common approach to the use of digital technologies and data in response to the current crisis. That approach should be effective in supporting competent national authorities, in particular health authorities and policy makers, by providing them with sufficient and accurate data to understand the evolution and spread of the COVID-19 virus as well as its effects. Similarly, these technologies may empower citizens to take effective and more targeted social distancing measures. At the same time, the proposed approach aims to uphold the integrity of the single market and protect fundamental rights and freedoms, particularly the rights to privacy and protection of personal data.

(4) Mobile applications can support health authorities at national and EU level in monitoring and containing the ongoing COVID-19 pandemic. They can provide guidance to citizens and facilitate the organisation of the medical follow-up of patients. Warning and tracing applications can play an important role in contact tracing, limiting the propagation of disease and interrupting transmission chains. Therefore, in combination with appropriate testing strategies and contact tracing, the applications can be particularly relevant in providing information on the level of virus circulation, in assessing the effectiveness of physical distancing and confinement measures, and in informing de-escalation strategies.

(5) Decision No 1082/2013/EU of the European Parliament and the Council[1] lays down specific rules on epidemiological surveillance, monitoring, early warning of, and combating serious cross-border threats to health. Article 2(5) of the Decision requires the Commission, in liaison with the Member States, to ensure coordination and information exchange between the mechanisms and structures established under that Decision and similar mechanisms and structures established at Union level or under the Euratom Treaty whose activities are relevant for preparedness and response planning, monitoring, early warning of, and combating serious cross-border threats to health. The forum for coordination of efforts in the context of serious cross-border threats to health is the Health Security Committee, set up by the Article 17 of the aforementioned Decision. At the same time, Article 6(1) of the Decision sets up a network for the epidemiological surveillance of communicable diseases, operated and coordinated by the European Centre for Disease Control.

(6) Directive 2011/24/EU of the European Parliament and of the Council[2] on the application of patients' rights in cross-border healthcare requires the eHealth Network to work towards delivering sustainable economic and social benefits of European eHealth systems and services and interoperable applications, with a view to achieving a high level of trust and security, enhancing continuity of care and ensuring access to safe and high-quality healthcare.

(7) Regulation (EU) 2016/679 of the European Parliament and of the Council[3] on the protection of natural persons with regard to the processing of personal data and on the free movement of such data lays down the conditions for processing personal data, including data concerning health. Such data may be processed *inter alia* when a data subject gives her explicit consent or when processing is in the public interest as specified in Member State or Union law, in particular for monitoring and alert purposes, the prevention or control of communicable diseases and other serious threats to health.

(8) Several Member States have introduced specific legislation that allow them to process health data, based on public interest (Article 6(1)(c) or (e) and Article 9(2)(i) of Regulation (EU) 2016/679). In any case, the purposes and means of the data processing, what data are to be processed and by whom, should be clear and specific.

(9) The Commission may consult the European Data Protection Supervisor and the European Data Protection Board, in accordance with Article 42 of Regulation (EU) 2018/1725 of the European Parliament and of the Council[4] and Article 70 of Regulation 2016/679.

---

1 Decision No 1082/2013/EU of the European Parliament and of the Council of 22 October 2013 on serious cross-border threats to health and repealing Decision No 2119/98/EC, OJ L 293, 5.11.2013, p. 1–15.

2 Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare, OJ L 88, 4.4.2011, p. 45–65.

3 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1–88.

4 Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, *OJ L 295, 21.11.2018, p. 39–98.*

(10) Directive 2002/58/EC of the European Parliament and of the Council[5] lays down the rules applicable to traffic and location data, and to the storing of information and the gaining of access to information stored in the terminal equipment, such as a mobile device, of a user or subscriber. Pursuant to Article 5(3) of the Directive, such storage or gaining of access is only permitted in narrowly defined circumstances or on the basis of consent of the user or subscriber, after having been provided with clear and comprehensive information, in accordance with the requirements of Regulation 2016/679. In addition, Article 15(1) of the Directive allows Member States to adopt legislative measures to restrict the scope of certain rights and obligations established by the Directive, including those set out in Article 5, when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to achieve certain objectives.

(11) The European Commission announced in its Communication, 'A European strategy for data'[6] that the EU would create a single market in which data can flow within the EU and across sectors, for the benefit of all, where European rules, in particular privacy and data protection, as well as competition law, are fully respected and where rules for access and use of data are fair, practical and clear. In particular, the Commission stated it would consider the need for legislative action to foster business-to-government data sharing for the public interest.

(12) Since the beginning of the COVID-19 crisis, a variety of mobile applications have been developed, some of them by public authorities, and there have been calls from Member States and the private sector for coordination at Union level, including to address cybersecurity, security and privacy concerns. These applications tend to serve three general functions: (i) informing and advising citizens and facilitating the organisation of medical follow-up of persons with symptoms, often combined with a self-diagnosis questionnaire; (ii) warning people who have been in proximity to an infected person in order to interrupt infection chains and preventing resurgence of infections in the reopening phase; and (iii) monitoring and enforcement of quarantine of infected persons, possibly combined with features assessing their health condition during the quarantine period. Certain applications are available to the general public, while others only to closed user groups directed at tracing contacts in the workplace. The effectiveness of these applications has generally not been evaluated. Information and symptom-checker apps may be useful to raise awareness of citizens. However, expert opinion suggests that applications aiming to inform and warn users seem to be the most promising to prevent the propagation of the virus, taking into account also their more limited impact on privacy, and several Member States are currently exploring their use.

---

5 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, p. 37–47, as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws., OJ L 337, 18.12.2009, p.11-36.

6 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A European strategy for data, COM/2020/66 final.

(13) Some of those mobile applications could be deemed medical devices where they are intended by the manufacturer to be used *inter alia* for diagnosis, prevention, monitoring, prediction, prognosis, treatment or alleviation of disease and would therefore fall within scope of under Regulation (EU) 2017/745 of the European Parliament and of the Council[7], or Council Directive 93/42/EEC[8]. For self-diagnosis and symptom-checker applications, where they provide information related to diagnosis, prevention, monitoring, prediction or prognosis, their potential qualification as medical devices according to the medical devices regulatory framework (Directive 93/42/EEC or Regulation (EU) 2017/745) should be assessed.

(14) The effectiveness of these mobile applications depends on a number of factors. Such factors include user penetration, that is, the percentage of the population using a mobile device and, of those, the percentage, who have downloaded the application and consented to the processing of personal data concerning them and not withdrawn that consent. Other important factors are public trust that the data will be protected by appropriate security measures, used exclusively to alert individuals who may have been exposed to the virus, public health authorities' endorsement, ability of the health authorities to take action based on the data generated by the application, integration and data sharing with other systems and applications, cross-border and cross-regional interoperability with other systems.

(15) Warning and tracing applications are useful for Member States for contact tracing purposes and can play an important role in containment during de-escalation scenarios. They can also be a valuable tool for citizens to practise effective and better targeted social distancing. Their impact can be boosted by a strategy supporting wider testing. Contact tracing implies that public health authorities rapidly identify all contacts of a confirmed COVID-19 patient, ask them to self-isolate, and rapidly test and isolate them if they develop symptoms. In addition, anonymised and aggregated data derived from such applications, combined with information on disease incidence, could be used to assess the effectiveness of community and physical distancing measures. While these applications are of evident usefulness for Member States, they also potentially add value to the work of the ECDC.

(16) Self-diagnoses and symptom checker applications could provide relevant information on the number of cases with COVID-19 compatible symptoms, by age and week, from well-defined areas where there is a high coverage of the application. If successful, national public health authorities can decide to use application data for COVID-19 syndromic primary care surveillance. These data could be provided to the ECDC weekly, in aggregated format (e.g. number of influenza-like illness (ILI) or acute respiratory infection (ARI) per week, by age group, out of the total population covered by the sentinel doctors). This would allow national authorities and the ECDC to estimate the positive predictive value of respiratory symptoms in a given community, thus providing information on the level of virus circulation based on the data from the application.

---

7 Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC, OJ L 117, 5.5.2017, p. 1–175.

8 Council Directive 93/42/EEC of 14 June 1993 concerning medical devices, OJ L 169, 12.7.1993, p. 1–43.

(17) Given the functions of smartphone applications as described above, their use is capable of affecting the exercise of certain fundamental rights such as *inter alia* the right to respect for private and family life. As any interference with those rights should be in accordance with the law, Member States' laws which would set out or permit limitations to the exercise of certain fundamental rights should be in line with the general principles of Union law as stated in Article 6 of the Treaty on the European Union, their constitutional traditions and their obligations under international law.

(18) For the acceptance of different types of applications (and underlying infection transmission chains information systems) and for ensuring that they fulfil the stated purpose of epidemiological surveillance, the underlying policies, requirements and controls must be aligned and implemented in a coordinated way by the responsible national health authorities. The experience of several Member States that started introducing contact tracing applications shows that, in order to increase the acceptance, an integrated governance is useful to prepare and implement the measures, involving not only health, but also other authorities (including data protection authorities), as well as the private sector, experts, academics and stakeholders such as patients groups. A wide communication concerning the application is also essential for its take-up and success.

(19) In order to detect proximity encounters between users of different contact tracing applications (a scenario most likely to happen among people moving across national/regional borders), interoperability between applications should be envisaged. National health authorities supervising infection transmission chains should be able to exchange interoperable information about users that have tested positive with other Member States or regions in order to address cross-border transmission chains.

(20) Certain companies including telecommunications providers and major technology platforms have published or made available to public authorities anonymised and aggregated location data. Such data is necessary for research to combat the virus, modelling to understand how the virus will spread and modelling of the economic effects of the crisis. In particular, the data will help to understand and model the spatial dynamics of the epidemic and to assess the impact of social distancing measures (travel limitations, non-essential activities closures, total lock-down etc.) on mobility. This is essential firstly to contain the effects of the virus and assess the needs notably in terms of Personal Protective Equipment and Intensive Care Units and, second, to support the exit strategy with data-driven models that indicate the potential effects of the relaxation of the social distancing measures.

(21) The current crisis has shown that public health authorities and research institutions would benefit from further access to essential information to analyse the evolution of the virus and to assess the effectiveness of public health measures.

(22) Certain Member States have taken measures to simplify access to necessary data. However, the EU's common efforts combating the virus are hampered by the current fragmentation of approaches.

(23) A common Union approach to the COVID-19 crisis has also become necessary since measures taken in certain countries, such as the geolocation-based tracking of individuals, the use of technology to rate an individual's level of health risk and the centralisation of sensitive data, raise questions from the viewpoint of several fundamental rights and freedoms guaranteed in the EU legal order, including the right to privacy and the right to the protection of personal data. In any event, pursuant to the Charter of Fundamental Rights of the Union, restrictions on the exercise of the

fundamental rights and freedoms laid down therein must be justified and proportionate. Any such restrictions should, in particular, be temporary, in that they remain strictly limited to what is necessary to combat the crisis and do not continue to exist, without an adequate justification, after the crisis has passed.

(24) Furthermore, the World Health Organisation and other bodies have warned of the risk that applications and inaccurate data could result in stigmatisation of persons who share certain characteristics because of a perceived link with the disease.

(25) In accordance with the principle of data minimization, public health authorities and research institutions should process personal data only where adequate, relevant and limited to what is necessary, and should apply appropriate safeguards such as pseudonymisation, aggregation, encryption and decentralization.

(26) Effective cybersecurity and data security measures are essential to protect the availability, authenticity integrity and confidentiality of data.

(27) Consultation with data protection authorities, in accordance with the requirements set out in Union law on the protection of personal data, is essential to ensure that personal data is processed lawfully and that the rights of the individuals concerned are respected.

(28) Article 14 of Directive 2011/24/EU[9] assigned the Union to support and facilitate cooperation and the exchange of information among Member States working within a voluntary network connecting national authorities responsible for eHealth designated by the Member States ('the eHealth Network'). Its objectives include working towards delivering sustainable economic and social benefits of European eHealth systems and services and interoperable applications, with a view to achieving a high level of trust and security, enhancing continuity of care and ensuring access to safe and high-quality healthcare. Commission Implementing Decision 2019/1765[10], lays down the rules for the establishment, management and transparent functioning of the eHealth Network. Because of its composition and area of expertise, the eHealth Network should be the main forum for discussions on the data needs of the public health authorities and research institutions, whilst also involving officials from national regulatory authorities for electronic communications, ministries in charge of digital matters and data protection authorities.

(29) The eHealth Network and the Commission should also closely co-operate with other bodies and networks that can provide the input necessary to give effect to this Recommendation, including the Health Security Committee, the network for the epidemiological surveillance of the communicable diseases, the ECDC, the European Data Protection Board, the Body of European Regulators for Electronic Communications and the Network Information Systems Cooperation Group.

(30) Transparency and clear and regular communication, and allowing for the input of persons and communities most affected, will be paramount to ensuring public trust when combating the COVID-19 crisis.

---

9 Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare, OJ L 88, 4.4.2011, p. 45.

10 Commission Implementing Decision 2019/1765 of 22 October 2019 providing the rules for the establishment, the management and the functioning of the network of national authorities responsible for eHealth, and repealing Implementing Decision 2011/890/EU (notified under document C(2019) 7460), OJ L 270, 24.10.2019, p. 83–93.

(31) Considering the rapid evolution of the situation in the various Member States in respect of the COVID-19 crisis, it is essential that Member States report and the Commission reviews the approach embodied in this Recommendation, quickly and regularly for as long as the crisis persists.

(32) This Recommendation should, where necessary, be complemented by additional guidance by the Commission, including on the data protection and privacy implications of the use of warn and prevent mobile applications.

HAS ADOPTED THIS RECOMMENDATION:

PURPOSE OF THIS RECOMMENDATION

(1) This recommendation sets up a process for developing a common approach, referred to as a Toolbox, to use digital means to address the crisis. The Toolbox will consist of practical measures for making effective use of technologies and data, with a focus on two areas in particular:

  (1) A pan-European approach for the use of mobile applications, coordinated at Union level, for empowering citizens to take effective and more targeted social distancing measures, and for warning, preventing and contact tracing to help limit the propagation of the COVID-19 disease. This will involve a methodology monitoring and sharing assessments of effectiveness of these applications, their interoperability and cross-border implications, and their respect for security, privacy and data protection; and

  (2) A common scheme for using anonymized and aggregated data on mobility of populations in order (i) to model and predict the evolution of the disease, (ii) to monitor the effectiveness of decision-making by Member States' authorities on measures such as social distancing and confinement, and (iii) to inform a coordinated strategy for exiting from the COVID-19 crisis.

(2) Member States should take these actions as a matter of urgency and in close coordination with other Member States, the Commission and other relevant stakeholders, and without prejudice to the competences of the Member States in the domain of public health. They should ensure that all actions are taken in accordance with Union law, in particular law on medical devices and the right to privacy and the protection of personal data along with other rights and freedoms enshrined in the Charter of Fundamental Rights of the Union. The Toolbox will be complemented by Commission guidance, including guidance on the data protection and privacy implications of the use of mobile warning and prevention applications.

DEFINITIONS

(3) For the purposes of this Recommendation:

(a) ‘Mobile applications’ means software application running on smart devices, in particular smartphones, designed usually for wide-ranging and targeted interaction with web resources, which process proximity data and other contextual information collected by many sensors found in any smart device and which are able to exchange information via many network interfaces with other connected devices;

(b) ‘eHealth Network’ means the network established by Article 14 of Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients’ rights in cross-border healthcare and whose tasks have been clarified by the Commission Implementing Decision 2019/1765 of 22 October 2019 providing the rules for the establishment, the management and the functioning of the network of national authorities responsible for eHealth, repealing the Commission Implementing Decision 2011/890/EU.

(c) ‘Health Security Committee’ means the body composed of representatives of the Member States, established under the article 17 of the Decision No 1082/2013/EU of the European Parliament and of the Council of 22 October 2013 on serious cross-border threats to health.

(d) ‘Epidemiological Surveillance Network’ means the network for the epidemiological surveillance of communicable diseases and of related special health issues operated and coordinated by the ECDC and bringing into permanent communication the Commission, the ECDC, and the competent authorities responsible at national level for epidemiological surveillance, set up under the article 6 of the Decision No 1082/2013/EU of the European Parliament and of the Council of 22 October 2013 on serious cross-border threats to health.

PROCESS FOR DEVELOPING A TOOLBOX FOR USE OF TECHNOLOGY AND DATA

(4) This process should facilitate the urgent development and adoption by Member States and the Commission of a toolbox of practical measures including a European approach for COVID-19 mobile applications and for the use of mobility data for modelling and predicting the evolution of the virus.

(5) For the development of the toolbox, Member States, represented in the eHealth Network, should meet, together with representatives of the Commission and the European Centre for Disease Control, immediately and frequently thereafter. They should share views on how best to use data from various sources to tackle the COVID-19 crisis whilst achieving a high level of trust and security in a manner compatible with Union law, in particular on the protection of personal data and privacy, as well as to share best practices and facilitate common approaches in that respect.

(6) The eHealth Network should meet immediately to operationalize this Recommendation.

(7) The Member States, represented in the eHealth Network, should, as appropriate, inform and seek input from the Health Security Committee, the Body of European Regulators for Electronic Communications, the NIS Cooperation Group and relevant

Commission agencies, including ENISA, Europol, and Council working groups, when giving effect to this Recommendation.

(8) The European Data Protection Board and the European Data Protection Supervisor should also be closely involved to ensure the Toolbox integrates data protection and privacy-by-design principles.

(9) Member States authorities and the Commission should ensure regular, clear and comprehensive communication to the public on the actions taken pursuant to this Recommendation and provide opportunities for the public to interact and participate in discussions.

(10) Paramount throughout the process should be respect for all fundamental rights, notably privacy as well as data protection, the prevention of surveillance and stigmatization. On these specific issues, the Toolbox should therefore:

(1) strictly limit the processing of personal data for the purposes of combating the COVID-19 crisis and ensure that the personal data are not used for any other purposes such as law enforcement or commercial purposes;

(2) ensure regular review of the continued need for the processing of personal data for the purposes of combating the COVID-19 crisis and set appropriate sunset clauses, so as to ensure that the processing does not extend beyond what is strictly necessary for those purposes;

(3) take measures to ensure that, once the processing is no longer strictly necessary, the processing is effectively terminated and the personal data concerned are irreversibly destroyed, unless, on the advice of ethics boards and data protection authorities, their scientific value in serving the public interest outweighs the impact on the rights concerned, subject to appropriate safeguards.

(11) The Toolbox should be developed progressively in the light of discussions with all interested parties and monitoring of the situation, best practice, issues and solution concerning the sources and types of data necessary and available for public health authorities and public health research institutions for combating the COVID-19 pandemic.

(12) The Toolbox should be shared with the European Union's international partners to exchange best practices and help address the virus spread worldwide.

A PAN-EUROPEAN APPROACH FOR COVID-19 MOBILE APPLICATIONS

(13) The first priority for the Toolbox should be a pan-European approach for COVID-19 mobile applications, to be developed together by Member States and the Commission, by 15 April 2020. The European Data Protection Board and the European Data Protection supervisor will be associated to the process. This approach should consist of:

(1) specifications to ensure the effectiveness of mobile information, warning and tracing applications for combating COVID-19 from the medical and technical point of view;

(2) measures to prevent proliferation of applications that are not compatible with Union law, to support requirements for accessibility for persons with disabilities, and for interoperability and promotion of common solutions, not excluding a potential pan-European application;

(3) governance mechanisms to be applied by public health authorities and cooperation with the ECDC;

(4) the identification of good practices and mechanisms for exchange of information on the functioning of the applications; and

(5) sharing data with relevant epidemiological public bodies and public health research institutions, including aggregated data to ECDC.

(14) Member State authorities, represented in the eHealth Network, should establish a process of exchanging information and ensuring interoperability of applications when cross-border scenarios are foreseen.

PRIVACY AND DATA PROTECTION ASPECTS OF USE OF THE MOBILE APPLICATIONS

(15) The development of the Toolbox should be guided by privacy and data protection principles.

(16) With particular regard the use of COVID-19 mobile warning and prevention applications, the following principles should be observed:

(1) safeguards ensuring respect for fundamental rights and prevention of stigmatization, in particular applicable rules governing protection of personal data and confidentiality of communications;

(2) preference for the least intrusive yet effective measures, including the use of proximity data and the avoidance of processing data on location or movements of individuals, and the use of anonymised and aggregated data where possible;

(3) technical requirements concerning appropriate technologies (e.g. Bluetooth Low Energy) to establish device proximity, encryption, data security, storage of data on the mobile device, possible access by health authorities and data storage;

(4) effective cybersecurity requirements to protect the availability, authenticity integrity, and confidentiality of data;

(5) the expiration of measures taken and the deletion of personal data obtained through these measures when the pandemic is declared to be under control, at the latest;

(6) uploading of proximity data in case of a confirmed infection and appropriate methods of warning persons who have been in close contact with the infected person, who shall remain anonymous; and

(7) transparency requirements on the privacy settings to ensure trust into the applications.

(17) The Commission will publish guidance further specifying privacy and data protection principles in the light of practical considerations arising from the development and implementation of the Toolbox.

USE OF MOBILITY DATA TO INFORM MEASURES AND EXIT STRATEGY

(18) The second priority for the Toolbox should be a common approach for the use of anonymised and aggregated mobility data necessary for:

(1) modelling to map and predict the diffusion of the disease and the impact on needs in the health systems in Member States, such as, but not limited, to Intensive Care Units in Hospitals and Personal Protective Equipment; and

(2) optimising the effectiveness of measures to contain the diffusion of the COVID-19 virus and to address its effects, including confinement (and de-confinement), and to obtain and use those data.

(19) In developing this approach, Member States (represented in the eHealth Network, which will coordinate with the Health Security Committee, the Epidemiological Network the ECDC and, if necessary, ENISA), should exchange best practices on the use of mobility data, share and compare modelling and predictions of the diffusion of the virus, and monitor the impact of measures to limit its diffusion.

(20) This deliverable should include:

(1) the appropriate use of anonymous and aggregated mobility data for modelling to understand how the virus will spread and modelling of the economic effects of the crisis;

(2) advice to public authorities on asking providers of the data for the methodology that they have applied for anonymising the data and to carry out a plausibility test of the methodology applied;

(3) safeguards to be put in place to prevent de-anonymisation and avoid re-identifications of individuals, including guarantees of adequate levels of data and IT security, and assessment of re-identification risks when correlating the anonymised data with other data;

(4) immediate and irreversible deletion of all accidentally processed data capable of identifying individuals and notifying the providers of the data as well as competent authorities of the accidental processing and deletion;

(5) deletion of the data in principle after a period of 90 days, or in any event no later than when the pandemic is declared under control; and

(6) restricting processing of the data exclusively for the purposes stated above and exclude sharing of the data with any third party.

REPORTING AND REVIEW

(21) The pan-European approach for COVID-19 mobile applications will be published on 15 April and will be complemented by Commission guidance on privacy and data protection.

(22) Member States should, by 31 May 2020, report to the Commission on the actions taken pursuant to this Recommendation. Such reports should continue on regular basis for as long as the COVID-19 crisis persists.

(23) As of 8 April 2020, Member States should make the measures applied in the areas covered by this Recommendation accessible to other Member States and to the Commission for peer review. Within one week, Member States and the Commission may submit observations on these measures. The Member State concerned should take utmost account of such observations.

(24) The Commission will, starting in June 2020, on the basis of these Member States reports, assess the progress made and the effect of this Recommendation. The Commission may make further recommendations to Member States, including on the timing of the measures applied in the areas covered by this Recommendation.

Done at Brussels, 8.4.2020

For the Commission
Thierry BRETON
Member of the Commission

CERTIFIED COPY
For the Secretary-General,

Jordi AYET PUIGARNAU
Director of the Registry
EUROPEAN COMMISSION