# Commission Implementing Decision (EU) 2020/1023 of 15 July 2020 amending Implementing Decision (EU) 2019/1765 as regards the cross-border exchange of data between national contact tracing and warning mobile applications with regard to combatting the COVID-19 pandemic (Text with EEA relevance)

## COMMISSION IMPLEMENTING DECISION (EU) 2020/1023

## of 15 July 2020

## amending Implementing Decision (EU) 2019/1765 as regards the cross-border exchange of data between national contact tracing and warning mobile applications with regard to combatting the COVID-19 pandemic

## (Text with EEA relevance)

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to 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[(1)], and in particular Article 14(3) thereof,

Whereas:

(1) Article 14 of Directive 2011/24/EU 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 (the 'eHealth Network') designated by the Member States.

(2) Commission Implementing Decision (EU) 2019/1765[(2)] provides for the rules for the establishment, the management and the functioning of the network of national authorities responsible for eHealth. Article 4 of that Decision entrusts the eHealth Network with the task of facilitating greater interoperability of the national information and communications technology systems and cross-border transferability of electronic health data in cross-border healthcare.

(3) In the light of the public health crisis caused by the COVID-19 pandemic, several Member States have developed mobile applications that support contact tracing and enable the users of such applications to be alerted to take appropriate action, such as testing or self-isolating, if they have been potentially exposed to the virus through proximity to another user of such applications, who has reported a positive diagnosis. These applications rely on Bluetooth technology to detect proximity between devices. As restrictions on travel between Member States have been lifted since June 2020, greater interoperability of the national information and communications technology systems should be achieved between the Member States in the eHealth Network, by implementing a digital infrastructure enabling interoperability between national mobile applications supporting contact tracing and warning.

(4) The Commission has been supporting Member States as regards the mobile applications mentioned above. On 8 April 2020, the Commission adopted a Recommendation 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 'Commission Recommendation')[3]. The Member States in the eHealth Network adopted, with the Commission's support, a Common EU toolbox for Member States on mobile applications to support contact tracing[4] as well as interoperability guidelines for approved contact tracing mobile applications in the EU[5]. The toolbox explains the national requirements for national contact tracing and warning mobile applications, in particular that they should be voluntary, approved by the respective national health authority, privacy-preserving, and dismantled as soon as no longer needed. Following the most recent developments of the COVID-19 crisis, the Commission[6] and the European Data Protection Board[7] have each issued guidance on mobile applications and contact tracing tools in relation to data protection. The design of Member States' mobile applications and of the digital infrastructure enabling their interoperability builds upon the Common EU toolbox, the above-mentioned guidance, and the technical specifications agreed in the eHealth Network.

(5) In order to facilitate the interoperability of national contact tracing and warning mobile applications, a digital infrastructure was developed with the support of the Commission by the Member States participating in the eHealth Network which decided to advance their cooperation in this area on a voluntary basis, as an IT tool for exchange of data. This digital infrastructure is referred to as 'the federation gateway'.

(6) This Decision lays down provisions on the role of the participating Member States and of the Commission for the functioning of the federation gateway for the cross-border interoperability of national contact tracing and warning mobile applications.

(7) Processing of personal data of application users of contact tracing and warning mobile applications, which is done under the responsibility of the Member States or other public organisations or official bodies in the Member States, should be carried out in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council[8] ('the General Data Protection Regulation') and Directive 2002/58/EC of the European Parliament and of the Council[9]. Processing of personal data under the responsibility of the Commission for the purpose of managing and ensuring the security of the federation gateway should comply with Regulation (EU) 2018/1725 of the European Parliament and of the Council[10].

(8) The federation gateway should consist of a secure IT infrastructure providing a common interface, where designated national authorities or official bodies can exchange a minimum set of data in relation to contacts with persons infected by SARS-CoV-2, in order to inform others on their potential exposure to that infection and promoting effective cooperation on healthcare between Member States by facilitating the exchange of relevant information.

(9) This Decision should therefore lay down modalities for the cross-border exchange of data between designated national authorities or official bodies through the federation gateway within the EU.

***Changes to legislation:** There are currently no known outstanding effects for the Commission Implementing Decision (EU) 2020/1023. (See end of Document for details)*

(10) The participating Member States, represented by the designated national authorities or official bodies determine together the purpose and means of processing of personal data through the federation gateway and are therefore joint controllers. Article 26 of the General Data Protection Regulation places an obligation on joint controllers of personal data processing operations to determine, in a transparent manner, their respective responsibilities for compliance with the obligations under that Regulation. It also provides for the possibility to have those responsibilities determined by Union or Member State law to which the controllers are subject. Each of the controllers should ensure that they have a legal basis at national level for processing in the federation gateway.

(11) The Commission, as a provider of technical and organisational solutions for the federation gateway, processes pseudonymised personal data on behalf of the participating Member States in the federation gateway as joint controllers and is therefore a processor. Pursuant to Article 28 of the General Data Protection Regulation and Article 29 of Regulation (EU) 2018/1725, the processing by a processor shall be governed by a contract or a legal act under Union or Member State law which is binding on the processor with regard to the controller and which specifies the processing. This Decision sets out rules on processing by the Commission as a processor.

(12) When processing personal data in the framework of the federation gateway, the Commission is bound by Commission Decision (EU, Euratom) 2017/46[11].

(13) Taking into account that the purposes for which controllers process personal data in the national contact tracing and warning mobile applications do not necessarily require the identification of a data subject, the controllers may not always be in a position to ensure the application of data subjects' rights. The rights referred to in Articles 15 to 20 of the General Data Protection Regulation may therefore not apply when the conditions pursuant to Article 11 of that Regulation are fulfilled.

(14) The existing Annex to Implementing Decision (EU) 2019/1765 needs to be renumbered due to the addition of two new annexes.

(15) Implementing Decision (EU) 2019/1765 should therefore be amended accordingly.

(16) Considering the urgency of the situation provoked by the COVID-19 pandemic, this Decision should apply from the day following that of its publication in the *Official Journal of the European Union*.

(17) The European Data Protection Supervisor was consulted in accordance with Article 42(1) of Regulation (EU) 2018/1725 and delivered an opinion on 9 July 2020.

(18) The measures provided for in this Decision are in accordance with the opinion of the Committee set up under Article 16 of Directive 2011/24/EU,

HAS ADOPTED THIS DECISION:

*Article 1*

Implementing Decision (EU) 2019/1765 is amended as follows:

**Changes to legislation:** *There are currently no known outstanding effects for the Commission Implementing Decision (EU) 2020/1023. (See end of Document for details)*

(1) in Article 2(1), the following points (g), (h), (i), (j), (k), (l), (m), (n) and (o) are inserted:

(g) "application user" means a person in possession of a smart device who has downloaded and runs an approved contact tracing and warning mobile application;

(h) "contact tracing" means measures implemented in order to trace persons who have been exposed to a source of a serious cross-border threat to health within the meaning of Article 3(c) of Decision No 1082/2013/EU of the European Parliament and of the Council[(12)];

(i) "national contact tracing and warning mobile application" means a software application approved at national level running on smart devices, in particular smartphones, designed usually for wide-ranging and targeted interaction with web resources, which processes proximity data and other contextual information collected by many sensors found in the smart devices for the purpose of tracing contacts with persons infected with SARS-CoV-2 and alerting persons who may have been exposed to SARS-CoV-2. These mobile applications are able to detect the presence of other devices using Bluetooth and exchange information with backend servers by using the internet;

(j) "federation gateway" means a network gateway operated by the Commission through a secure IT tool that receives, stores and makes available a minimum set of personal data between Member States' backend servers for the purpose of ensuring the interoperability of national contact tracing and warning mobile applications;

(k) "key" means a unique ephemeral identifier related to an application user reporting to have been infected with SARS-CoV-2, or who may have been exposed to SARS-CoV-2;

(l) "verification of infection" means the method applied for confirming an infection with SARS-CoV-2, namely whether this was self-reported by the application user or resulted from confirmation from a national health authority or a laboratory test;

(m) "countries of interest" means the Member State, or Member States, where an application user has been in the 14 days prior to the date of upload of the keys and where he has downloaded the approved national contact tracing and warning mobile application and/or has travelled;

(n) "country of origin of the keys" means the Member State where the backend server that uploaded the keys to the federation gateway is located;

(o) "log data" means an automatic record of an activity in relation to the exchange of, and access to, data processed through the federation gateway, that show in particular the type of processing activity, the date and time of the processing activity, and the identifier of the person processing the data.;

(2) in Article 4(1), the following point (h) is inserted:

(h) provide guidance to the Member States on the cross-border exchange of personal data through the federation gateway between national contact tracing and warning mobile applications.;

(3) in Article 6(1), the following points (f) and (g) are inserted:

(f) develop, implement and maintain appropriate technical and organisational measures related to the security of transmission and hosting of personal data in the federation gateway for the purpose of ensuring the interoperability of national contact tracing and warning mobile applications;

(g) support the eHealth Network in agreeing on the technical and organisational compliance of the national authorities with the requirements for the cross-border exchange of personal data in the federation gateway by providing and carrying out the necessary tests and audits. Experts from the Member States may assist the Commission auditors.;

(4) Article 7 is amended as follows:

(a) the title is replaced by 'Protection of personal data processed through the eHealth Digital Service Infrastructure';

(b) in paragraph 2 'Annex' is replaced by 'Annex I';

(5) the following Article 7a is inserted:

*Article 7a*

**Cross-border exchange of data between national contact tracing and warning mobile applications through the federation gateway**

1 Where personal data is exchanged through the federation gateway, the processing shall be limited to the purposes of facilitating the interoperability of national contact tracing and warning mobile applications within the federation gateway and the continuity of contact tracing in a cross-border context.

2 The personal data referred to in paragraph 3 shall be transmitted to the federation gateway in a pseudonymised format.

3 The pseudonymised personal data exchanged through and processed in the federation gateway shall only comprise the following information:

a the keys transmitted by the national contact tracing and warning mobile applications up to 14 days prior to the date of upload of the keys;

b log data associated to the keys in line with the technical specifications protocol used in the country of origin of the keys;

c the verification of infection;

d the countries of interest and the country of origin of the keys.

4 The designated national authorities or official bodies processing personal data in the federation gateway shall be joint controllers of the data processed in the federation gateway. The respective responsibilities of the joint controllers shall be allocated in accordance with Annex II. Each Member State wishing to participate in the cross-border exchange of data between national contact tracing and warning mobile applications shall notify the Commission, prior to joining, of its intention and indicate the national authority or official body that has been designated as the responsible controller.

5 The Commission shall be the processor of personal data processed within the federation gateway. In its capacity as processor, the Commission shall ensure the security of processing, including the transmission and hosting, of personal data within