II

(Non-legislative acts)

DECISIONS

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.

([1]) OJ L 88, 4.4.2011, p. 45.

([2]) Commission Implementing Decision (EU) 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 (OJ L 270, 24.10.2019, p. 83).

(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.

([3]) Commission Recommendation (EU) 2020/518 of 8 April 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 (OJ L 114, 14.4.2020, p. 7).

([4]) https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf

([5]) https://ec.europa.eu/health/sites/health/files/ehealth/docs/contacttracing_mobileapps_guidelines_en.pdf

([6]) Communication from the Commission, Guidance on Applications supporting the fight against COVID 19 pandemic in relation to data protection (OJ C 124I, 17.4.2020, p. 1).

([7]) Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak and EDPB statement of 16 June 2020 on the data protection impact of the interoperability of contact tracing apps, both available at: https://edpb.europa.eu

([8]) 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).

([9]) 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).

([10]) 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).

(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:

(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 (*);

([11]) Commission Decision (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission (OJ L 6, 11.1.2017, p. 40). The Commission publishes further information on Security standards applying to all European Commission information systems on https://ec.europa.eu/info/publications/security-standards-applying-all-european-commission-information-systems_en

(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.

_____

(*) 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).';

(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 the federation gateway and shall comply with the obligations of a processor laid down in Annex III.

6. The effectiveness of the technical and organisational measures for ensuring the security of processing of personal data within the federation gateway shall be regularly tested, assessed and evaluated by the Commission and by the national authorities authorised to access the federation gateway.

7. Without prejudice to the decision of the joint controllers to terminate the processing in the federation gateway, the operation of the federation gateway shall be deactivated at the latest 14 days after all the connected national contact tracing and warning mobile applications cease to transmit keys through the federation gateway.';

(6) the Annex becomes Annex I;

(7) Annexes II and III are added, the text of which is set out in the Annex to this Decision.

Article 2

This Decision shall enter into force on the day following that of its publication in the *Official Journal of the European Union*.

Done at Brussels, 15 July 2020.

For the Commission
The President
Ursula VON DER LEYEN

ANNEX

In Implementing Decision (EU) 2019/1765, the following Annexes II and III are added:

'ANNEX II

RESPONSIBILITIES OF THE PARTICIPATING MEMBER STATES AS JOINT CONTROLLERS FOR THE FEDERATION GATEWAY FOR CROSS-BORDER PROCESSING BETWEEN NATIONAL CONTACT TRACING AND WARNING MOBILE APPLICATIONS

SECTION 1

Subsection 1

Division of responsibilities

(1) The joint controllers shall process personal data through the federation gateway in accordance with the technical specifications stipulated by the eHealth Network ([1]).

(2) Each controller shall be responsible for the processing of personal data in the federation gateway in accordance with the General Data Protection Regulation and Directive 2002/58/EC.

(3) Each controller shall set up a contact point with a functional mailbox that will serve for the communication between the joint controllers and between the joint controllers and the processor.

(4) A temporary subgroup set up by the eHealth network in accordance with Article 5(4) shall be tasked to examine any issues arising from the interoperability of national contact tracing and warning mobile applications and from the joint controllership of related processing of personal data and to facilitate coordinated instructions to the Commission as a processor. Amongst other issues, the controllers may, in the framework of the temporary subgroup, work towards a common approach on the retention of data in their national backend servers, taking into account the retention period set forth in the federation gateway.

(5) Instructions to the processor shall be sent by any of the joint controllers' contact point, in agreement with the other joint controllers in the subgroup referred to above.

(6) Only persons authorised by the designated national authorities or official bodies may access personal data of users exchanged in the federation gateway.

(7) Each designated national authority or official body shall cease to be joint controller from the date of withdrawal of its participation in the federation gateway. It shall however remain responsible for processing in the federation gateway that occurred prior to its withdrawal.

Subsection 2

Responsibilities and roles for handling requests of and informing data subjects

(1) Each controller shall provide the users of its national contact tracing and warning mobile application ("the data subjects") with information about the processing of their personal data in the federation gateway for the purposes of cross-border interoperability of the national contact tracing and warning mobile applications, in accordance with Articles 13 and 14 of the General Data Protection Regulation.

(2) Each controller shall act as the contact point for the users of its national contact tracing and warning mobile application and shall handle the requests relating to the exercise of the rights of data subjects in accordance with the General Data Protection Regulation, submitted by those users or their representatives. Each controller shall designate a specific contact point dedicated to requests received from data subjects. If a joint controller receives a request from a data subject, which does not fall under its responsibility, it shall promptly forward it to the responsible joint controller. If requested, the joint controllers shall assist each other in handling data subjects' requests and shall reply to each other without undue delay and at the latest within 15 days from receiving a request for assistance.

([1]) In particular, the interoperability specifications for cross-border transmission chains between approved apps, of 16 June 2020, available at: https://ec.europa.eu/health/ehealth/key_documents_en#anchor0

(3) Each controller shall make available to the data subjects the content of this Annex including the arrangements laid down in points 1 and 2.

SECTION 2

Management of security incidents, including personal data breaches

(1) The joint controllers shall assist each other in the identification and handling of any security incidents, including personal data breaches, linked to the processing in the federation gateway.

(2) In particular, the joint controllers shall notify each other of the following:

a) any potential or actual risks to the availability, confidentiality and/or integrity of the personal data undergoing processing in the federation gateway;

b) any security incidents that are linked to the processing operation in the federation gateway;

c) any personal data breach, the likely consequences of the personal data breach and the assessment of the risk to the rights and freedoms of natural persons, and any measures taken to address the personal data breach and mitigate the risk to the rights and freedoms of natural persons;

d) any breach of the technical and/or organisational safeguards of the processing operation in the federation gateway.

(3) The joint controllers shall communicate any personal data breaches with regard to the processing operation in the federation gateway to the Commission, to the competent supervisory authorities and, where required so, to data subjects, in accordance with Articles 33 and 34 of Regulation (EU) 2016/679 or following notification by the Commission.

SECTION 3

Data Protection Impact Assessment

If a controller, in order to comply with its obligations specified in Articles 35 and 36 of the General Data Protection Regulation needs information from another controller, it shall send a specific request to the functional mailbox referred to in Subsection 1(3) of Section 1. The latter shall use its best efforts to provide such information.

ANNEX III

RESPONSIBILITIES OF THE COMMISSION AS DATA PROCESSOR FOR THE FEDERATION GATEWAY FOR CROSS-BORDER PROCESSING BETWEEN NATIONAL CONTACT TRACING AND WARNING MOBILE APPLICATIONS

The Commission shall:

(1) Set up and ensure a secure and reliable communication infrastructure that interconnects national contact tracing and warning mobile applications of the Member States participating in the federation gateway. To fulfil its obligations as data processor of the federation gateway, the Commission may engage third parties as sub-processors; the Commission shall inform the joint controllers of any intended changes concerning the addition or replacement of other sub-processors thereby giving the controllers the opportunity to jointly object to such changes as set out in Annex II, Subsection 1(4) of Section 1. The Commission shall ensure that the same data protection obligations as set out in this Decision apply to these sub-processors.

(2) Process the personal data, only based on documented instructions from the controllers, unless required to do so by Union or Member State law; in such a case, the Commission shall inform the controllers of that legal requirement before processing, unless that law prohibits submitting such information on important grounds of public interest.

(3) The processing by the Commission entails the following:

a) Authentication of national backend servers, based on national backend server certificates;

b) Reception of the data referred to in Article 7a, paragraph 3, of the Implementing Decision uploaded by national backend servers by providing an application programming interface that allows national backend servers to upload the relevant data;

c) Storage of the data in the federation gateway, upon receiving them from national backend servers;

d) Making the data available for download by national backend servers;

e) Deletion of the data when all participating backend servers have downloaded them or 14 days after their reception, whichever is earlier.

f) After the end of the provision of service, delete any remaining data unless Union or Member State law requires storage of the personal data.

The processor shall take the necessary measures to preserve the integrity of the data processed.

(4) Take all state of the art organisational, physical and logical security measures to maintain the federation gateway. To this end, the Commission shall:

a) designate a responsible entity for the security management at the level of the federation gateway, communicate to the controllers its contact information and ensure its availability to react to security threats;

b) assume the responsibility for the security of the federation gateway;

c) ensure that all individuals that are granted access to the federation gateway are subject to contractual, professional or statutory obligation of confidentiality;

(5) Take all necessary security measures to avoid compromising the smooth operational functioning of the national backend servers. To this end, the Commission shall put in place specific procedures related to the connection from the backend servers to the federation gateway. This includes:

a) risk assessment procedure, to identify and estimate potential threats to the system;

b) audit and review procedure to:

   i. check the correspondence between the implemented security measures and the applicable security policy;

   ii. control on a regular basis the integrity of system files, security parameters and granted authorisations;

   iii. monitor to detect security breaches and intrusions;

   iv. implement changes to mitigate existing security weaknesses

   v. allow for, including at the request of controllers, and contribute to, the performance of independent audits, including inspections, and reviews on security measures, subject to conditions that respect Protocol (No 7) to the TFEU on the Privileges and Immunities of the European Union ([2]);

([2]) Protocol (No 7) on the Privileges and Immunities of the European Union (OJ C 326, 26.10.2012, p. 266).

c) changing the control procedure to document and measure the impact of a change before its implementation and keep the controllers informed of any changes that can affect the communication with and/or the security of their infrastructures;

d) laying down a maintenance and repair procedure to specify the rules and conditions to be respected when maintenance and/or repair of equipment should be performed;

e) laying down a security incident procedure to define the reporting and escalation scheme, inform without delay the controllers, as well as the European Data Protection Supervisor of any personal data breach and define a disciplinary process to deal with security breaches.

(6) Take state of the art physical and/or logical security measures for the facilities hosting the federation gateway equipment and for the controls of logical data and security access. To this end, the Commission shall:

a) enforce physical security to establish distinct security perimeters and allowing detection of breaches;

b) control access to the facilities and maintain a visitor register for tracing purposes;

c) ensure that external people granted access to the premises are escorted by duly authorised staff;

d) ensure that equipment cannot be added, replaced or removed without prior authorisation of the designated responsible bodies;

e) control access from and to the national backend servers to the federation gateway;

f) ensure that individuals who access the federation gateway are identified and authenticated;

g) review the authorisation rights related to the access to the federation gateway in case of a security breach affecting this infrastructure;

h) keep the integrity of the information transmitted through the federation gateway;

i) implement technical and organisational security measures to prevent unauthorised access to personal data;

j) implement, whenever necessary, measures to block unauthorised access to the federation gateway from the domain of the national authorities (i.e.: block a location/IP address).

(7) Take steps to protect its domain, including the severing of connections, in the event of substantial deviation from the principles and concepts for quality or security.

(8) Maintain a risk management plan related to its area of responsibility.

(9) Monitor – in real time – the performance of all the service components of its federation gateway services, produce regular statistics and keep records.

(10) Provide support for all federation gateway services in English, 24/7 via phone, mail or Web Portal and accept calls from authorised callers: the federation gateway's coordinators and their respective helpdesks, Project Officers and designated persons from the Commission.

(11) Assist the controllers by appropriate technical and organisational measures, insofar as it is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the General Data Protection Regulation.

(12) Support the controllers by providing information concerning the federation gateway, in order to implement the obligations pursuant to Articles 32, 35 and 36 of the General Data Protection Regulation.

(13) Ensure that data processed within the federation gateway is unintelligible to any person who is not authorised to access it.

(14) Take all relevant measures to prevent that the federation gateway's operators have unauthorised access to transmitted data.

(15) Take measures in order to facilitate the interoperability and the communication between the federation gateway's designated controllers.

(16) Maintain a record of processing activities carried out on behalf of the controllers in accordance with Article 31(2) of Regulation (EU) 2018/1725.'