EDPS comments on the Commission draft implementing decision amending Implementing Decision 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

1. Introduction

Context of the draft Proposal

- The eHealth Network is a voluntary network of responsible authorities for eHealth designated by Member States. The network is provided in Article 14 of Directive 2011/24/EU on patients' rights in cross border healthcare.[1] Commission Implementing Decision 2019/1765[2] sets out the rules and the establishment, management and functioning of the eHealth network. Among others, one of the main objectives of the eHealth network is to enhance interoperability of the national information and communications technology systems and cross-border transferability of electronic health data in cross-border healthcare. In this framework, the eHealth network and the Commission have developed an IT tool, namely the eHealth Digital Service Infrastructure ('eHDSI'), in order to exchange health data under the Connecting Europe Facility programme[3], also developed by the Commission. It is worth recalling that the EDPS and the EDPB have issued a Joint Opinion 1/2019 on the processing of patients' data and the role of the European Commission within the eHDSI[4].

- In the light of the public health crisis caused by the COVID-19 pandemic, EU Member States have developed mobile applications that support contact tracing and warning. 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 develop an IT tool for exchange of data, namely 'the federation gateway'.

- In the context of contact tracing applications, 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

[1] 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 88/45.
[2] 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 (OJ L 270, 24.10.2019).
[3] Regulation (EU) No 1316/2013 of the European Parliament and of the Council of 11 December 2013 establishing the Connecting Europe Facility, amending Regulation (EU) No 913/2010 and repealing Regulations (EC) No 680/2007 and (EC) No 67/2010, OJ L 348, 20.12.2013.
[4] EDPB-EDPS Joint Opinion 1/2019 on the processing of patients' data and the role of the European Commission within the eHealth Digital Service Infrastructure (eHDSI), 15 July 2019, https://edps.europa.eu/sites/edp/files/publication/19-07-15_edpb_edps_joint_opinion_ehealth_en.pdf .

and the use of anonymised mobility data (the 'Commission Recommendation')[5]. 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[6] as well as interoperability guidelines for approved contact tracing mobile applications in the EU[7]. Following the most recent developments of the COVID-19 crisis, the Commission[8] and the European Data Protection Board have issued guidance on mobile applications and contact tracing tools in relation to data protection and interoperability.[9]

- 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. The 'federation gateway' aims to provide a secure IT infrastructure providing a common interface, where designated national authorities or official bodies would exchange a minimum set of data in relation to contacts with persons infected by SARS-CoV-2, with the objective of informing others on their potential exposure to that infection and promoting effective cooperation on healthcare between Member States by facilitating the exchange of relevant information.

- The draft Commission Implementing Decision aims at laying down provisions on the role of the 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, while also identifying the modalities for the cross-border exchange of data between designated national authorities or official bodies through the federation gateway within the EU.

Scope of the comments

- The present comments concern the draft Commission Implementing Decision amending Implementing Decision 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, together with its Annex (which provides two additional annexes to Implementing Decision 2019/1765).

- The comments are issued pursuant to Article 42(1) Regulation (EU) 2018/1725, following a request for consultation from the European Commission of 6 July 2020.

2. The EDPS Comments

2.1. General comments

[5] 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).
[6] https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf.
[7] https://ec.europa.eu/health/sites/health/files/ehealth/docs/contacttracing_mobileapps_guidelines_en.pdf.
[8] 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).
[9] 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.

- The EDPS welcomes the decision of the Commission to define the roles of the actors involved in the cross-border exchange of data between national contact tracing and warning mobile applications combatting the COVID-19 pandemic. The EDPS also welcomes that the draft Implementing Decision contains an Annex (composed of two Annexes) providing for the allocation of responsibilities of Member States (as joint controllers) and the Commission (as processor) for the processing of personal data within the federation gateway. The EDPS notes, however, that in certain areas the Annexes mainly refer to or replicate the provisions of the GDPR, and therefore considers that further specification would be needed. Without seeking to be exhaustive, the comments below provide a number of recommendations in this respect.

2.2. The designation of joint controllers and processor

- Article 7a of the draft Implementing Decision provides that "*[t]he 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."* On the other hand, *"[t]he Commission shall be the processor of personal data processed within the federation gateway. (...)"* The responsibilities of the joint controllers and the processor are further defined in Annexes II and III respectively.

- As mentioned above, the EDPS and the EPDB have already provided a joint Opinion on the roles and responsibilities of Member States and Commission in the processing of personal data within the eHDSI. The Opinion found that "*(...) even though the Commission is involved in some of the procedures regarding the development of technical and organisational solutions, as well as the systems' security elements, it does not have decision making power in terms of defining the purpose or the essential means related to this processing operation*". It followed that, given the legal framework related to the definition of the purposes and means of the infrastructure, and given the strict limitations of the Commission's tasks to ensure the security of the core services of the eHDSI, the Commission was considered as a processor acting on behalf of the Member States for eHealth when carrying out the processing of patients' data.[10]

- In this specific context, the EDPS is of the view that the assessment on the roles of the parties involved does not substantially differ from the one done in the context of the processing of personal data within the eHDSI. Both the purposes and means of the processing operation taking place within the federation gateway are decided by the eHealth Network: the purpose of the federation gateway is to facilitate the interoperability of national contact tracing and warning mobile applications, while the means of the processing operation taking place within the federation gateway are decided by the Member States in the eHealth Network.[11] The Commission would again provide its guidance (a function in itself compatible with the one of a processor under data protection law), act as the provider of technical and organisational solutions for the federation gateway, processing only pseudonymised personal data on behalf of the participating Member States.

[10] https://edps.europa.eu/sites/edp/files/publication/19-07-15_edpb_edps_joint_opinion_ehealth_en.pdf

[11] See also the technical specifications stipulated by the eHealth Network (available at https://ec.europa.eu/health/ehealth/key_documents_en#anchor0). In accordance with Annex II, Section 1, Subsection 1 of the Draft Implementing Decision "*[t]he joint controllers shall process personal data through the federation gateway in accordance with the technical specifications stipulated by the eHealth Network*".

- The EDPS notes that point 6 of Article 7a of the draft Implementing Decision could be interpreted as limiting the security obligation of the processor to "hosting and transmission". In accordance with Article 33 of Regulation 2018/1725, the processor is required to ensure the security of all processing it carries out on behalf of the controller. For the avoidance of doubt, the EDPS recommends replacing the words "of the transmission and of the hosting" by "of processing, including the transmission and hosting".

2.3. Responsibilities of the joint controllers (Annex II)

Section 1

Subsection 1 - Division of responsibilities

- Article 26(1) of the GDPR provides that joint controllers shall in a transparent manner determine and agree on their respective responsibilities for compliance with the obligations under the Regulation. The determination of their respective responsibilities is to be carried out by joint controllers "*in particular"* as regards the exercising of the rights of the data subject and the duties to provide information referred in Articles 13 and 14, unless and in so far as the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject.

- It follows from the wording of Article 26 that the distribution of the responsibilities for compliance among joint controllers is not limited to the rights of the data subject and the duties to provide information, but should also cover other controller obligations as necessary to ensure that the whole joint processing fully complies with the GDPR. The EDPS welcomes the fact that several additional obligations are already considered in Annex II of the draft Implementing Decision. In the sections that follow, the EDPS provides a number of recommendations to render the division of responsibilities more comprehensive.

- Point 2 provides that *"[E]ach controller shall be responsible for the processing of personal data in the federation gateway in accordance with Articles 5, 24 and 26 of the General Data Protection Regulation and Directive 2002/58/EC.*" As a general rule, the GDPR shall be applicable in its entirety to each of the joint controllers. The EDPS recommends the Commission to either provide further clarification as to why Articles 5, 24 and 26 of the GDPR are listed in particular, or to delete this point entirely, as the GDPR shall in any event be applicable to the joint controllers.

- Point 5 states that "*Instructions to the processor shall be sent by any of the joint controllers' contact point, in agreement with the other joint controllers.*" The Annex does not specify further how agreement among the joint controllers shall be reached. The EDPS recommends clarifying how this decision would be made. If this were to be taken by the eHealth Network, we recommend adding a specific reference to any document providing for details on the decision-making process within the network.

Subsection 2 - Responsibilities and roles for handling requests of and informing data subjects

- Point 1 provides that each controller shall provide the users of its national contact tracing and warning mobile application 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. The EDPS recalls that at the latest at the time when personal data are obtained by the controller(s), the data subject needs to be given clear information about the additional processing related to ensuring of interoperability.[12]

- Point 2 provides that each joint controller shall act as the contact point for the users of its national contact tracing and warning mobile application. It also provides that 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.

- The EDPS recalls that pursuant to Article 26(3) of the GDPR, irrespective of the terms of the arrangement among joint controllers, the data subject may exercise his or her rights under this Regulation in respect of and against each of the controllers. In other words, it is not sufficient for a joint controller to merely forward the request from the data subject to the responsible data controller. It must also ensure that adequate follow-up is provided.

- To facilitate matters, the EDPS recommends identifying a specific contact point dealing with such request and ensuring this is made manifest to data subjects.[13] This would not only provide more clarity and transparency of information to data subjects, but could also guarantee that adequate follow-up is provided to each request.[14]

2.4. Processor responsibilities (Annex III)

- Point 1 stipulates that, in case of sub-processing, 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. The EDPS recommends to further clarify how the joint controllers would "jointly object" in practice. If such a joint objection were to be taken in the context of the eHealth Network, we recommend adding a specific reference to any document providing for details on the decision-making process within the network.

- Point 3 e) provides that the processing by the Commission will entail that data shall be deleted when all participating backend servers have downloaded them or 14 days after their reception, whichever is earlier. The processing of data for interoperability purposes should also allow for the definition for common retention periods for all Member States as well. Therefore, it is recommended that the period of the 14 days in total shall also be applied, when the data have been downloaded to the national backend servers and

[12] See also EDPB statement of 16 June 2020 on the data protection impact of the interoperability of contact tracing apps, paragraphs 9-11.
[13] See the EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation 2018/1725, available at https://edps.europa.eu/sites/edp/files/publication/19-11-07_edps_guidelines_on_controller_processor_and_jc_reg_2018_1725_en.pdf
[14] Such an approach would also be in line with the EDPB guidance stipulating that any interoperable solution needs to facilitate away for data subjects to exercise their rights. Where the exercise of rights is possible, it should not become more cumbersome for the data subjects and it should be clear to whom the data subjects should turn to exercise their rights. EDPB statement of 16 June 2020 on the data protection impact of the interoperability of contact tracing apps, paragraph 16.

should not be kept for longer period. The EDPS recommends to clarify this issue in the text of the Annex.

- Pursuant to point 5, the Commission should put in place specific procedures related to the connection from the backend servers to the federation gateway, which include, *inter alia*, "define the conditions under which to authorise, including at the request of controllers, and contribute to, the performance of independent audits, including inspections, and reviews on security measures." In this respect, the EDPS draws attention to Article 29(3)(h) of Regulation 2018/1725, that requires the processor to allow for and contribute to audits, including inspections conducted by the controller or another auditor mandated by the controller.

- Finally, in its statement the EDPB stresses that *"[W]hen providers are considering how to make their contact tracing applications interoperable, they should as far as possible ensure that this does not lead to a lowering of the level of data quality or accuracy*."[15] In this regard, the EDPS recommends to explicitly address measures for preserving data quality or accuracy in Annex III (3).

Brussels, 9 July 2020

[15] EDPB statement of 16 June 2020 on the data protection impact of the interoperability of contact tracing apps, paragraph 19.