EUROPEAN DATA PROTECTION SUPERVISOR

EDPS Orientations on manual contact tracing by EU Institutions in the context of the COVID-19 crisis

Executive Summary

Some European institutions, agencies and bodies (EUIs) have implemented a manual contact tracing system in order to trace persons who have been in close contact with a person infected by COVID-19. Contact tracing shall assist medical staff to assess the spread of a contagious disease and if possible prevent additional infection.

The EDPS considers that manual contact tracing is compatible with the requirements of Regulation (EU) 2018/1725 (the Regulation) as long as EUIs put in place comprehensive data protection measures. The ethics of public health information requires that privacy considerations are thoroughly addressed at all levels of contact tracing activities.

Article 10(2)(b) and10(2)(h) of the Regulation are relevant lawful grounds for the processing of special categories of personal data for the manual contact tracing of staff and members of the staff's household. The provisions of Article 59 of the Staff Regulation related to the management of medical leave is the relevant legal ground for the processing of COVID-19 medical information by the medical service of EUI. Article 59(5) of the Staff Regulations satisfy the requirement of lawfulness for contact tracing, including the collection of data from members of the staff's household, provided that such information is disclosed by the staff member.

The EDPS observes that EUIs do not have a legal basis, comparable to Article 59(5) of the Staff Regulations, to process health related data of non-staff person in its manual contact tracing operation. However, the EDPS considers that informing a non-staff person that he or she may have been in contact with an individual who has been found to be infected can be considered as a processing necessary for the performance of a task carried out in the public interest under Article 5(1)(a) of the Regulation. The lawfulness of this limited processing operation (restricted to informing the non-staff person) can be established by Article 1(e)(2) of the Staff Regulations supplemented with an executive decision of an EUI, agency or body providing for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

In view of the high sensitivity of the data at stake and the high risk for the privacy of individuals, EUIs need to conduct a DPIA when developing and implementing a manual contact tracing operation. By performing a DPIA, controllers will be able to design a robust and data protection-compliant system that will contribute to the smooth deployment of such system and its operational success.

Informing affected data subjects should be done on the basis of a clear protocol limiting the amount of data to what it is considered strictly necessary to achieve its goals. Additionally, adequate security measures following Article 33 of the Regulation need to be in place when information and communication technologies are used for this purpose. The implementation of a manual contact tracing process by EUIs requires specific and adequate safeguards under Article 10 of the Regulation. The EUI shall take steps to ensure that any person acting under his authority process the data under its specific instructions.

Table of Contents

1 Introduction

In addition to other mitigation measures such as teleworking and compulsory body temperature measurement at the entrance of their buildings, some European institutions, agencies and bodies (EUIs) have implemented a manual contact tracing system in order to trace persons who have been in close contact with a person infected by COVID-19. Other EUIs might follow and apply a similar measure.

EUIs put in place manual contact tracing systems to fight the COVID-19 pandemic within the European institutions as part of their standard epidemiological toolkit. Contact tracing shall assist medical staff to assess the spread of a contagious disease and if possible prevent additional infection by isolating contact persons before being contagious and thus spreading themselves the disease.

The EDPS considers that manual contact tracing is compatible with the requirements of Regulation (EU) 2018/1725[1] (the Regulation) as long as EUIs put in place comprehensive data protection measures. The ethics of public health information requires that privacy considerations are thoroughly addressed at all levels of contact tracing activities[2].

The EDPS distinguishes between manual contact tracing and contact tracing with mobile applications. Manual contact tracing relies on health service agents to survey contaminated individuals for their close contacts. Subsequently, the health service agents reach out to those close contacts in order to assess their risks of having being infected and spreading the disease. They provide mitigation advice such as the need to undergo a test, inform their close contacts or quarantine/self-isolate.

With the wide availability of mobile phones, mobile applications have been developed during this health crisis in order to notify the users on possible infection risks and assist health authorities in identifying and informing contact persons. The EDPS has already presented an overview of contact tracing with mobile applications in May 2020[3]. In addition, the European Data Protection Board (EDPB) has also published in April 2020 comprehensive guidelines on such tools[4].

Due to its very different nature and data protection concerns, the issues raised by such system is not discussed in this document which is solely focused on manual contact tracing.

2 Legal measures in relation to manual contact tracing

2.1 Scope

Manual contact tracing is implemented at Member State level by the respective national health authorities. The system is broadly designed by national health authorities around persons living or entering the country. These authorities benefit from a well-defined public health legal framework with robust protocols related to the management of contagious diseases.

Except for some specialised agencies like the European Centre for Disease Prevention and Control ('ECDC') that regularly or exclusively work in this domain, some EUIs, due to the COVID-19 crisis, only recently started developing a manual contact tracing system aiming mainly to protect the health of their employees and their contacts.

Manual contact tracing is an epidemiological tool designed to break the chain of contamination. While contact tracing is primarily linked to persons with a confirmed diagnosis of COVID-19 infection, other data subjects, who are not currently infected or confirmed to be infected, are

also concerned by this processing activity. Thus, this tracing system developed by EUIs will primarily concern their staff, although it could also concern other persons, who regularly work within or occasionally visit the EUI building, but are not directly employed by EUIs such as cleaning agents, experts from the Member State or security staff (non-staff). In addition, it may involve tracing members of the staff's household (i.e.: wife, children, parents…).

2.2 Legal basis

Most health and safety measures adopted by EUIs during this COVID-19 crisis are designed to provide a safe working environment for its staff in application of the requirements set out in Article 1(e)(2) of the Staff Regulation[5]. The provision of masks or the measurement of body temperature are passive systems intended to reduce the infection risk.

Manual contact tracing actively contribute to the medical management of an epidemic, an activity which fall outside the primary role of EUIs except for specific institutions working in this domain.

All processing operations must satisfy the requirement of lawfulness as set out in Articles 5 and 10 (for health data) of the Regulation.

Given the employment context of such tracing system, it is unlikely that consent would provide a valid or a relevant legal ground for the processing operation[6]. The EDPS considers relevant to distinguish the collection and processing of personal data from staff and members of the staff's household from the processing of personal data of non-staff persons.

2.2.1 Staff and members of the staff's household

The EDPS considers that Article 10(2)(b) and10(2)(h) of the Regulation are relevant lawful grounds for the processing of special categories of personal data for the manual contact tracing of staff and members of the staff's household.

The provisions of Article 59 of the Staff Regulation related to the management of medical leave is the relevant legal ground for the processing of COVID-19 medical information by the medical service of EUI. However, it only applies to staff members who have a confirmed diagnosis.

Article 59(5) of the Staff Regulations providing that an "[o]fficial may be required to take leave after examination by the institution's medical officer if his state of health so requires or if a member of his household is suffering from a contagious disease." satisfy the requirement of lawfulness for contact tracing, including the collection of data from members of the staff's household, provided that such information is disclosed by the staff member. However, it is the EDPS understanding that Article 59(5) is not applicable to staff members who will not generate a chain of contamination at the office (e.g. members who are exclusively teleworking and has not come to the office at all in the period during which they were contagious).When a staff member from one EUI may have been in contact with an infected person from another EUI, there is a need to share the tracing information between different EUIs' medical services. Such transmission of personal data would need to comply with the Regulation and is further discussed in section 3.3.

Manual contact tracing is subject to the principle of proportionality. Only relevant data, adequate and limited to what is necessary for the purpose (data minimisation) shall be collected and processed. Only those persons in close contact with the infected staff member shall be traced and monitored.

Given the exponential nature of the infection dynamic, if the contamination level is too widespread within EUIs, the EDPS believes that the most appropriate measure to break the contamination chain would be, as it is the case at the moment of the adoption of these orientations, the extensive use of teleworking for most staff members and drastically limiting the amount of close contacts staff would encounter at work.

In any case, following the dynamic nature of the contagion, EUIs must regularly review the use of such tool and its proportionality.

2.2.2 Non-staff person

During normal day-to-day operation, EUIs may collect personal data such as access register or meeting lists of non-staff contacts regularly or occasionally visiting EUIs premises. This data might, incidentally, be of interest for contact tracing operations.

The EDPS observes that **EUIs do not have a legal basis, comparable to Article 59(5) of the Staff Regulations, to process health related data of non-staff person in its manual contact tracing operation**. However, the EDPS considers that informing a non-staff person that he or she may have been in contact with an individual who has been found to be infected can be considered as a processing necessary for the performance of a task carried out in the public interest under Article 5(1)(a) of the Regulation. The lawfulness of this limited processing operation (restricted to informing the non-staff person) can be established by Article 1(e)(2) of the Staff Regulations supplemented with an executive decision of an EUI, agency or body providing for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject. In this case, the processing should be strictly limited to the purpose of informing the non-staff contacts and providing him/her with the contact details of local health authorities. EUIs should not collect medical or health related information from a non-staff person aside from the information required to contact trace its staff. Non-staff persons should be clearly informed that access register or meeting lists may be used for contact tracing.

EUIs may also collaborate with employers of non-staff contacts persons in order to have a comprehensive contact tracing system.

Similarly, employers of non-staff persons, especially those who regularly work within EUIs buildings, should inform the EUIs of any employees being infected and equally respect the right to privacy and anonymity of their own employee. In other words, they should provide the necessary information for EUIs to identify his own staff who is at risk.

This information might be legitimately transmitted to national health authorities provided that the requirements described in section 3.4 are met. **Local health authorities are normally entitled to know the infection status of non-staff contacts and should collaborate with the EUIs' health service. Likewise, local health authorities may provide information to EUI medical service in order to trace staff members who have been in contact with infected non-staff contacts.** This does not prevent EUIs to trace contacts of its staff following the lawful disclosure of a contact with someone infected.

2.3 The need for a data protection impact assessment

Given the ramifications on data subject's privacy of contact tracing, it is relevant to analyse whether a data protection impact assessment (DPIA) is required under Article 39 of the Regulation. In accordance with Article 39(4), the EDPS has published on 17 July 2019 a decision which provides a framework for EUIs as controller to assess when it is necessary to conduct a DPIA for a processing operation[7]. In this decision, various criteria are deemed "(...) likely to result in a high risk to the rights and freedoms of natural persons". A toolkit is provided in annex 1 of this decision in order to assist EUIs in undergoing this analysis. The following criteria would apply for a manual contact tracing processing operation implemented by EUIs.

The first applicable criterion is the use of sensitive data concerning the health of the data subject. Contact tracing is triggered when it is discovered that the data subject is contaminated or possibly contaminated by the COVID-19 disease.

The second applicable criterion is the potential scale of the manual contact tracing operation. COVID-19 disease can potentially infect anyone and thus should a large number of concerned data subjects be infected, the scale of the manual contact tracing operation could include a large number of staff members as well as staff members of other EUIs and numerous non-staff persons who were in close contact with infected or possibly infectious persons. While some data subjects may have a limited range of contacts, others given the global influence of the operation of the European Union could have been in close contact with a large number persons that would need to be traced.

Finally, a third criterion should also be considered. It will be the first time that EUIs implement a manual contact tracing operation. It will involve the application of novel organizational solution and processes. As shown for example in section 3.2, badly designed procedures and unidentified data flows may lead to accidental exposure of sensitive medical data that may not only affect the data subject but also the global acceptance of this kind of operation. For its success, it is essential that the main data protections risks and issues are properly identified and addressed for this novel processing operation. A comprehensive DPIA will assist EUIs and provide a framework to tackle them.

In view of the high sensitivity of the data at stake and the high risk for the privacy of individuals, EUIs need to conduct a DPIA when developing and implementing a manual contact tracing operation. By performing a DPIA, controllers will be able to design a robust and data protection-compliant system that will contribute to the smooth deployment of such system and its operational success.

3 Operational aspects of manual contact tracing

3.1 Medical data for medical professional

Given the nature of the pandemic, COVID-19 infections are not exceptional. Still, the infection status remains sensitive health data that require special care even if data subjects commonly share this information within their social circle.

As shown above, the relevant legal ground for the processing of health data related to the COVID-19 infection by EUIs is Article 59(5) of the Staff Regulation. This Article clearly indicates that "**the institution's medical officer**" is playing a critical role in processing the information linked to contact tracing. Therefore, the processing of health data should remain under the control and supervision of the medical officer or other medical professionals who are

bound by medical confidentiality. Contact persons should preferably be contacted by personnel able to provide relevant information regarding the contamination risk and guidance on mitigation measures and treatment option.

Special care should be applied when communicating health related information to non-medical staff in order to implement the relevant mitigation measures. EUIs must ensure that only the necessary information is provided. For instance, for the disinfection of an office, it is sufficient to designate which offices need to be fully cleaned. It is paramount to preserve the confidentiality of the medical information of the affected staff. This requirement does not prevent the processing of non-medical or health related data by non-medical staff but in charge of security or relevant measures in order to implement general health and safety measures.

3.2 Communication to the contact persons

A vital step of manual contact tracing is informing the contact persons of a positive test of COVID-19. As such, this process can be disturbing for the privacy of the affected persons and their close contacts and special attention should be given to provide such information in a discreet way, respecting data protection rules.

Informing affected data subjects should be done on the basis of a clear protocol limiting the amount of data to what it is considered strictly necessary to achieve its goals. Additionally, adequate security measures following Article 33 of the Regulation need to be in place when information and communication technologies are used for this purpose.

Information provided in the context of contact tracing must:

- not reveal the identity of persons with a confirmed diagnosis of Covid-19 infection to the contact persons,
- avoid informing simultaneously different contacts of a person (e.g. by putting them in cc of the email notification), as this could result in revelation of the person's contacts and to a violation of his/her data protection rights.
- refrain from including other, non-necessary, information about the affected persons, such as information on their health conditions or additional contact details that could identify the affected individual.

The EUIs should regularly remind staff members involved in the contact tracing operation of the sensitivity of the personal data being processed and of the common mistakes that can occur especially with the use of communication technologies (such as email, SMS etc).

In case of a security incident during the above process which is identified as a personal data breach, the DPO of the EUI should immediately be involved in order to advise on measures to limit the impact of the incident. Due to the sensitivity of the personal data involved in this process, apart from notifying the breach to the EDPS, the EUI should inform affected data subjects according to Article 35 of the Regulation.

3.3 Communication between medical officers of various EUIs

During the normal operation of EUIs, staff members of different EUIs meet regularly for various reasons. In case of an infected staff member, EUIs may consider to trace or inform contacts of other EUIs. In order to implement an effective manual contact tracing strategy, EUIs as controllers need to transmit personal data to EUIs whose staff was in contact with the infected or potentially infected person. In such case, EUIs must comply with the requirements of Recital 21 of the Regulation[8] and ensure that the transmitted information is necessary for the implementation of an effective contact tracing strategy.

Medical services should agree how to proceed in practice with these data exchanges with appropriate technical and organisational measures to guarantee the confidentiality of the transmission of data.

If bigger EUIs propose the use of their contact tracing platform to smaller EUIs, the responsibilities of each party in this processing operation should be clarified. Such relationships also need to comply with the requirements of either Article 28 (joint controller) or 29 (processor) of the Regulation[9].

3.4 Data transmission with local health authority

As previously mentioned, manual contact tracing by EUIs should be mainly limited to their staff and members of their household. Yet, the COVID-19 disease is not limited to the professional environment and local health authority will probably request data from contaminated staff members in order to expand the contact tracing operation to the full social sphere of the infected individual. This data transmission needs to comply with the requirements of Article 9 of the Regulation.

Provided that the local health authority establishes that the request for transmission of personal data of the infected person falls within its legal duties to implement a contact tracing operation, it shall comply with the requirements of Article 9 (1)(a) of the Regulation.

In any case, EUIs as controller need to ensure that the personal data transmitted to the local health authority is limited to what is necessary to pursue a local contact tracing strategy. In addition, EUIs must implement proper security measures in order to safeguard the confidentiality of the information provided.

3.5 Duration of data storage

Controllers are reminded that the data collected for contact tracing need to be stored only for the required amount of time needed to achieve the primary goal of such processing operation and thus to comply with the requirements of Article 4 (1)(e). Thus following the complete tracing of the contacts of the affected data subject, the data collected for this specific purpose should be stored for a maximum of 14 days then be deleted in due time.

While, the use of the manual contact tracing system for other purpose (“function creep”) must be avoided, it does not prevent the storage of such data for other compatible legitimate and duly documented medical or epidemiological purposes. If the collected data is meant to be used for research or statistical purpose, it is advised that safeguards designed to comply with Article 13 of the Regulation are implemented right at the start of the processing operation.

3.6 Technical and organisational measures

The implementation of a manual contact tracing process by EUIs requires specific and adequate safeguards under Article 10 of the Regulation. The security of the data in the whole data cycle of the process shall be ensured following the application of the adequate measures according Article 33 of the Regulation. The EUI shall take steps to ensure that any person acting under his authority process the data under its specific instructions.

As for any data processing operation, **data protection by design and by default** set out in Article 27 of the Regulation must be applied. EUIs must ensure that they safely collect and process only the minimum amount of data and use privacy-friendly technologies at all stages of the process. This may include:

- Providing access only on a need-to-know-basis to agents briefed about confidentiality,

- Implementing accountability measures with regards to data access (e.g. logging),

- Storing the contact data on secured servers or on cloud services designed for storing health data.

The implemented measures should be documented and regularly audited.

Great care should be taken in relation to the collected health data and controllers should use enhanced protection measures such as encryption. Similar security measures should be implemented for data transmission between various EUIs medical services and also with local public health authority in order to guarantee the confidentiality of the transmitted personal data.

A full **data life cycle analysis** as required with DPIA can assist controllers in identifying weak spots and operational risks in the processing operation.

The purpose of this system must solely remain the disruption of contamination chain within EUIs.

3.7 Data subject's rights

The medical imperatives of the management of the spread of the COVID-19 disease within the EUIs does not preclude controllers to comply with the requirement of Chapter 3 of the Regulation (Rights of data subject).

For instance, if there is any question on how the manual contact tracing system works and what data are collected, data subjects should be able to receive appropriate information from the data controller and have controller's contact details for lodging complaints or giving feedback on the contact tracing system. In particular, controllers should provide clear information to data subjects as regard to the collaboration between EUI and local public health authority.

In addition, controllers should also provide clear information to the data subjects in relation to the possibility to oppose the contact tracing operation and its consequences. If there are any restrictions to the data subject's rights, they must comply with the requirements of Article 25 of the Regulation.

[1] 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 (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1725)

[2]See for instance World Health Organization (WHO) interim Guidance of 10 may 2020 on "Contact tracing in the context of Covid-19", available here: https://www.who.int/publications/i/item/contact-tracing-in-the-context-of-covid-19 and the WHO Guidelines on ethical issues in public health surveillance of 2017, available here: https://www.who.int/ethics/publications/public-health-surveillance/en/ .

[3]*TechDispatch #1/2020: Contact Tracing with Mobile Applications* found on https://edps.europa.eu/data-protection/our-work/publications/techdispatch/techdispatch-12020-contact-tracing-mobile_en

[4] *EDPB guideline 04/2020 of 21 April 2020 on contact tracing tool* found on https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf

[5] *"Officials in active employment shall be accorded working conditions complying with appropriate health and safety standards at least equivalent to the minimum requirements applicable under measures adopted in these areas pursuant to the Treaties. »*. This provision should be interpreted with the requirements set out in Directive (89/391/EEC) on the introduction of measures to encourage improvements in the safety and health of workers at work and in particular Article 6.

[6] For further analysis, you may read page 9 of the European Data Protection Board's Guidelines 05/2020 on consent under Regulation 2016/679.

[7] Found at https://edps.europa.eu/data-protection/our-work/publications/guidelines/data-protection-impact-assessment-list_en

8

In accordance with the principle of accountability, where Union institutions and bodies transmit personal data within the same Union institution or body and the recipient is not part of the controller, or to other Union institutions or bodies, they should verify whether such personal data are required for the legitimate performance of tasks within the competence of the recipient. In particular, following a recipient's request for transmission of personal data, the controller should verify the existence of a relevant ground for lawfully processing personal data and the competence of the recipient. The controller should also make a provisional evaluation of the necessity of the transmission of the data. If doubts arise as to this necessity, the controller should seek further information from the recipient. The recipient should ensure that the necessity of the transmission of the data can be subsequently verified.

[9] In this regard, see EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725, https://edps.europa.eu/sites/edp/files/publication/19-11-07_edps_guidelines_on_controller_processor_and_jc_reg_2018_1725_en.pdf .