
# Statement on the data protection impact of the interoperability of contact tracing apps

## Adopted on 16 June 2020

**The European Data Protection Board has adopted the following statement:**

1. In the Guidelines 04/2020[1] on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, the EDPB encouraged having "a common European approach in response to the current crisis, or at least put in place an interoperable framework."

2. The EDPB has taken note of the interoperability guidelines for approved contact tracing mobile applications in the EU, adopted by the eHealth network on 13 May 2020[2], which describes interoperability in the context of contact tracing applications as

> "being able to exchange *the minimum information necessary* so that individual app users, wherever they are located in the EU, are alerted if they have been in proximity, within a relevant period, with another user who has notified the app that he/she has tested positive for COVID-19." (Emphasis added.)

3. The Interoperability guidelines further state that the alert and follow up should be in accordance with the procedures defined by public health authorities with potential privacy and security implications assessed and appropriate safeguards applied.

4. In this statement, the EDPB further elaborates on the level of impact on the right to data protection that an interoperable implementation can entail, depending on the implementation. Any recommendations made in this statement are in addition to those made in the EDPB Guidelines 04/2020, which remain applicable.

---

[1] https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042020-use-location-data-and-contact-tracing_en

[2] https://ec.europa.eu/health/sites/health/files/ehealth/docs/contacttracing_mobileapps_guidelines_en.pdf - Please note that this is a living document and subject to change by the European Commission (See page 3 of the version of 13 May 2020)

## General considerations

5. Firstly, the EDPB would like to recall that the use of contract tracing applications relies on the processing of pseudonymised personal data of the users of the applications.[3] This includes health data, for instance whenever a user has been confirmed positive by a health care professional or when exposure information is processed by the system. Analogously to what was said on the general use of contact tracing applications[4], the EDPB is of the view that enabling of the sharing of data about individuals that have been diagnosed or tested positively ("infection data") with such interoperable applications should only be triggered by a voluntary action of the user. Data subjects[5] need to be in control of their data. The goal of interoperability should not be used as an argument to extend the collection of personal data beyond what is necessary.

6. In general, the interoperability of contact tracing applications within EEA may increase their effectiveness in supporting already existing measures in place as, irrespective of the app used, the tracing of more possible contacts and potential alerts will be possible. It will simplify the use especially for individuals in border regions, when travelling or when working in jobs or areas that may expose them to many people from other Member States (e.g. for tourism). However, given the potential increased data protection risk arising from interoperability, discussed below, controllers should also explore other alternatives.

7. Moreover, as is true for the applications themselves, such solutions would need to be part of a comprehensive public health strategy to fight the pandemic, including, inter alia, testing and subsequent manual contact tracing for the purpose of improving effectiveness of the performed measures.

8. The EDPB is aware of contact tracing applications with different underlying approaches in the different Member States and acknowledges that ensuring interoperability of different implementations is technically challenging and may require substantial financial and engineering effort. To ensure the minimum exchange and processing of data, as is required by the GDPR, contact tracing application developers will need to agree on a common protocol and compatible data structures. Thus, for applications already sharing a common framework or at least the same technology basis, the goal of interoperability may be easier to achieve than for those that do not. In fact, due to the differences between the approaches, it may in practice prove infeasible to implement interoperability without disproportionate trade-offs.

## Key issues

### Transparency

9. Interoperability will lead to additional processing and disclosure of data to additional entities. As always, data subjects need to be made aware of any additional processing of their personal data and the involved parties.[6] The users should always have a clear understanding of what the use of the application entails and should remain in control of their data.

---

[3] See Recital 26 GDPR which specifies what is to be considered as personal data
[4] Hereinafter synonymous with the term "apps" and "applications".
[5] Hereinafter synonymous with the term user.
[6] See as well: Article 29 Working Party: "Guidelines on transparency under Regulation 2016/679", WP260 rev.01, 11 April 2018 - endorsed by the EDPB.

10. 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 the use of interoperability. At this point the user needs to be informed of the conditions and extent of the data processing.

11. Standard rules for transparency are still applicable; the information should be provided in clear and plain language.[6] This includes information on how the data that is shared will be processed by the receiving interoperable contact tracing application.

## Legal basis

12. The same legal bases as discussed in the Guidelines 04/2020 are still applicable. When relying on public interest, national law may need to be adjusted to provide for the sharing of the data with other services. In case of consent, an additional consent will need to be collected for the interoperability processing fulfilling all of its requirements. In particular, it needs to be specific and therefore sufficiently granular.[7] When different legal bases are used by the different data controllers of the contact tracing applications, additional measures may be required to implement data subject rights related to the legal basis. Where it concerns health data Art. 9 GDPR is applicable and the controllers will need to be able to rely on one of the exceptions mentioned there.

## Controllership

13. The EDPB would like to clarify that a definitive statement regarding the respective roles of the different actors involved in any processing needs a specific assessment on a factual basis on how the processing is carried out. However, the EDPB would like to stress the importance to carefully consider these roles and responsibilities when designing a solution. The following can therefore only serve as a guidance of a general nature.

14. In the opinion of the EDPB any operation or set of operations that pursue the purpose of ensuring the interoperability in addition to the processing for the functionality of applications on Member State level has to be assessed separately from prior or subsequent processing operations because of the additional purpose. Therefore, this additional processing should be seen as a separate processing. For this separate processing operation, the parties may be individual controllers or joint controllers, who may use processors. Any subsequent processing undertaken after the exchange of the identifiers (calculating exposure, alerting identified contacts, etc.) would happen under separate controllership by the receiving application provider.

15. The respective roles, relationships and responsibilities of the joint controllers in regards to the data subject will need to be defined and this information should then be made available to the data subject.[8] This will have an impact on the scope of the DPIA that needs to be performed, including the processing performed for the purpose of interoperability. The processing for the purpose of ensuring the interoperability may be entrusted to a processor meeting the conditions of Art 28 GDPR.

[7] See also Section 3.1.3 Granularity of the EDPB Guidelines 05/2020 on consent under Regulation 2016/679

[8] The EDPB will expand on joint controllership in its upcoming Guidelines on the concepts of controller and processor in the GDPR

### Exercise of data subject rights

16. Any interoperable solution needs to facilitate a way 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. Limitations to the exercise of data subject rights are possible under the exemptions stipulated in Art 11[9] and Art 23 GDPR.

### Data retention and minimisation

17. Differences in the set data retention period should not lead to data being stored for longer than what is necessary.[10] In order to promote the effective application of data protection principles, a common level of data minimisation and a common data retention period should be considered. As mentioned before, interoperability should not lead to an increased collection of information due to a lack of a coordinated approach. This will need to be clearly communicated to the user before sharing the data.

### Information Security

18. Interoperability should not lead to a decrease in data security and the protection of personal data. The EDPB recommends that the providers of contact tracing applications take into consideration any increase in information security risks caused by the additional processing and the involvement of additional actors. This notably concerns security of data in transit for the possible interconnection of back-end servers. In particular, measures addressing security risks related to interoperability that have an impact on the rights and freedoms of natural persons must be addressed in the DPIA.

### Data Accuracy

19. When 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. Interoperability, in case of large divergences may lead to a loss of data quality (e.g. incorrect assessment conclusions, poor assignment of risk rating), which could lead to an increase of false positives. These additional risks to data accuracy will need to be clearly communicated to the data subjects.

20. Measures put in place to ensure data accuracy need to be maintained in the interoperable system.

## Conclusion

21. The EDPB is aware that creating an interoperable network of applications is not trivial. While this may increase their effectiveness it could as well require major changes to applications already in place or under development. From a data protection point of view, interoperability is possible if the recommendations in this statement as well as those in the EDPB Guidelines 04/2020[1] are followed. Giving data subjects information and control will increase their trust in the solutions and its potential uptake.

---

[9] As pointed out under the General Considerations, interoperability will entail processing of pseudonymised personal data

[10] See as well the EDPB Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak

22. Contact tracing applications can only be a temporary solution as part of a comprehensive public health strategy to fight the current pandemic. For each introduced measure, it needs to be assessed whether a less intrusive alternative can achieve the same purpose, and ensured that any measure applied is effective and proportionate.

For the European Data Protection Board

The Chair

(Andrea Jelinek)