Statement on the processing of personal data in the context of reopening of borders following the COVID-19 outbreak

Adopted on 16 June 2020

The European Data Protection Board has adopted the following statement:

1. In the Communication from the Commission on the third assessment of the application of the temporary restriction on non-essential travel to the EU from 11 June 2020, the Schengen Member States and Schengen Associated States are invited to lift internal border controls by 15 June 2020 and to prolong the temporary restriction on non-essential travel into the EU until 30 June 2020. The communication also sets out an approach to progressively lifting the restriction afterwards which is in line with the Joint European Roadmap towards lifting COVID-19 measures, agreed on by the European Council 26 March 2020.

2. In this context, on 15 June 2020 some Member States have started the progressive lifting of the measures taken to fight the COVID-19 pandemic, including restrictions to the free movements of persons within the internal market and the Schengen area, as well as to the entrance of citizens from third countries through the external borders of the EU. The plans for progressive lifting incorporate measures whose purpose is to control the flow of individuals entering into and/or travelling within the EEA territory. Similar national measures are being taken by the EEA/EFTA Member States of the EDPB, as Schengen Associated States.

3. While the EDPB is fully aware of the relevance of the fundamental right to health, the said measures cannot in any case suppose an erosion of the persons' fundamental rights and freedoms and of the right to data protection in particular. This statement is therefore based on the attempt to strike the balance between the fundamental rights at stake in the context of the current COVID-19 pandemic.

4. The opening of borders is in part made possible by processing different types of personal data at the borders. In general, the purpose of the processing is to prevent and control the pandemic by mitigating risk factors with certain measures. The measures currently envisaged or implemented by Member States include, for example, testing for COVID-19, requiring certificates issued by health professionals

and the use of a voluntary contact tracing app.[1] Most measures involve some level of processing of personal data. The categories of data collected can be, for example, contact details, health data and location data.

5. As previously stated by the EDPB, data protection does not impede the fight against the COVID-19 pandemic. The data protection legislation remains applicable and allows for an efficient response to the pandemic, while at the same time protecting fundamental rights and freedoms. Data Protection law, including relevant applicable national law, already enables data processing operations necessary to contribute to the fight against the spread of a pandemic, such as the COVID-19 pandemic.

6. Therefore, the EDPB urges the Member States to take a common European approach when deciding which processing of personal data is necessary to ensure that the risk of the pandemic spreading is mitigated, while respecting the fundamental rights and freedoms of individuals. When deciding what measures are necessary, Member States must respect the fundamental rights as described in the Charter, to privacy and data protection, as well general data protection rules. The EDPB emphasises that the processing of personal data in this context must be necessary and proportionate. In the light of these principles, measures should also be based on scientific evidence. Furthermore, the EDPB recalls that the protection of personal data must be ensured consistently throughout the Union/EEA, wherever data subjects are situated.

7. More specifically the EDPB emphasises that certain aspects of the data protection legislation require special attention by Member States, i.e.:

- **Lawfulness, fairness and transparency.** The processing of data entailed in the decided measures must be transparent and fair towards the data subject and be based on proper legal basis in Article 6 and when special categories of data are processed Article 9 of the GDPR. Furthermore, relevant and appropriate information should be given to the data subject in clear and easily accessible manner.

- **Purpose limitation**. The processing should be limited to the purpose of combating the COVID-19 pandemic, preventing the spread of the pandemic across borders and to facilitate the provision of necessary health care. Purpose should be specified for every data controller and processing operations.

- **Data minimisation**. Member States should only process data that are adequate, accurate, relevant and limited to what is necessary in relation to the defined purpose for which they are processed.

- **Storage limitation.** Member States should ensure that data are only kept for short period of time and in any case, no longer than is necessary for the purpose of the processing.

- **Security of the data.** Member States should ensure the appropriate level of security by implementing appropriate technical and organisational measures to secure the data, based on a risk assessment, for example by using pseudonymisation and an appropriate level of encryption, when processing data of a highly personal nature, such as health and location data.

[1] See Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak and Statement on the data protection impact of the interoperability of contact tracing apps.

- **Data Protection by design and by default and Data Protection Impact Assessment**. Member States should implement Data Protection by design and by default principles along with, when applicable, a data protection impact assessment[2].

- **Sharing of personal data.** Processors of personal data should only receive personal data when a data processing agreement is in place. Member States should, when applicable, clearly define the responsibilities between the public authority who acts as data controller and the data processor in such an agreement in accordance with Article 28 of the GDPR. Sharing data with other controllers should only take place if there is an appropriate legal basis.

- **Automated individual decision making.** The decision to allow the entrance into a country should not only be based on the available technology. In any case, such decision should be subject to suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision. Such measure should not concern a child.

8. Finally, the EDPB stresses the **importance of a prior consultation with competent national data protection authorities when Member States process personal data in this context**, in order to facilitate the correct application of the data protection legislation.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

[2] See: Article 29 Working Party Guidelines on Data Protection Impact Assessment (DPIA) (wp248rev.01) - endorsed by the EDPB