



Statement of the EDPB Chair on the processing of personal data in the context of the COVID-19 outbreak

Brussels, 16 March 2020 – Governments, public and private organisations throughout Europe are taking measures to contain and mitigate COVID-19. This can involve the processing of different types of personal data.

Andrea Jelinek, Chair of the European Data Protection Board (EDPB), said: “Data protection rules (such as GDPR) do not hinder measures taken in the fight against the coronavirus pandemic. However, I would like to underline that, even in these exceptional times, the data controller must ensure the protection of the personal data of the data subjects. Therefore, a number of considerations should be taken into account to guarantee the lawful processing of personal data.”

The GDPR is a broad legislation and also provides for the rules to apply to the processing of personal data in a context such as the one relating to COVID-19. Indeed, the GDPR provides for the legal grounds to enable the employers and the competent public health authorities to process personal data in the context of epidemics, without the need to obtain the consent of the data subject. This applies for instance when the processing of personal data is necessary for the employers for reasons of public interest in the area of public health or to protect vital interests (Art. 6 and 9 of the GDPR) or to comply with another legal obligation.

For the processing of electronic communication data, such as mobile location data, additional rules apply. The national laws implementing the ePrivacy Directive provide for the principle that the location data can only be used by the operator when they are made anonymous, or with the consent of the individuals. The public authorities should first aim for the processing of location data in an anonymous way (i.e. processing data aggregated in a way that it cannot be reversed to personal data). This could enable to generate reports on the concentration of mobile devices at a certain location (“cartography”).

When it is not possible to only process anonymous data, Art. 15 of the ePrivacy Directive enables the member states to introduce legislative measures pursuing national security and public security¹. This emergency legislation is possible under the condition that it constitutes a necessary, appropriate and proportionate measure within a democratic society. If such

¹ In this context, it shall be noted that safeguarding public health may fall under the national and/or public security exception.

measures are introduced, a Member State is obliged to put in place adequate safeguards, such as granting individuals the right to judicial remedy.