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

Adopted on 19 March 2020

The European Data Protection Board has adopted the following statement:

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.

Data protection rules (such as the GDPR) do not hinder measures taken in the fight against the coronavirus pandemic. The fight against communicable diseases is a valuable goal shared by all nations and therefore, should be supported in the best possible way. It is in the interest of humanity to curb the spread of diseases and to use modern techniques in the fight against scourges affecting great parts of the world. Even so, the EDPB would like to underline that, even in these exceptional times, the data controller and processor 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 and in all cases it should be recalled that any measure taken in this context must respect the general principles of law and must not be irreversible. Emergency is a legal condition which may legitimise restrictions of freedoms provided these restrictions are proportionate and limited to the emergency period.

1. Lawfulness of processing

The **GDPR is a broad piece of legislation and provides for rules that also apply to the processing of personal data in a context such as the one relating to COVID-19**. **The GDPR allows competent public health authorities and employers to process personal data in the context of an epidemic, in accordance with national law and within the conditions set therein**. For example, when processing is necessary for reasons of substantial public interest in the area of public health. Under those circumstances, there is no need to rely on consent of individuals.

1.1 With regard to the processing of personal data, including special categories of data by competent public authorities (e.g. public health authorities), the EDPB considers that articles 6 and 9 GDPR enable the processing of personal data, in particular when it falls under the legal mandate of the public authority provided by national legislation and the conditions enshrined in the GDPR.

1.2 In the employment context, the processing of personal data may be necessary for compliance with a legal obligation to which the employer is subject such as obligations relating to health and safety at the workplace, or to the public interest, such as the control of diseases and other threats to health.

The GDPR also foresees derogations to the prohibition of processing of certain special categories of personal data, such as health data, where it is necessary for reasons of substantial public interest in the area of public health (Art. 9.2.i), on the basis of Union or national law, or where there is the need to protect the vital interests of the data subject (Art.9.2.c), as recital 46 explicitly refers to the control of an epidemic.

1.3 With regard to the processing of telecom data, **such as location data**, national laws implementing the ePrivacy Directive must also be respected. In principle, location data can only be used by the operator when made anonymous or with the consent of individuals. However, Art. 15 of **the ePrivacy Directive enables Member States to introduce legislative measures to safeguard public security.** Such exceptional legislation is only possible **if it** constitutes a **necessary, appropriate and proportionate measure within a democratic society**. These measures must be in accordance with the Charter of Fundamental Rights and the European Convention for the Protection of Human Rights and Fundamental Freedoms. Moreover, it **is subject to the judicial control of the European Court of Justice and the European Court of Human Rights.** In case of an emergency situation, it should also be strictly limited to the duration of the emergency at hand.

2. Core principles relating to the processing of personal data

Personal data that is necessary to attain the objectives pursued should be processed for specified and explicit purposes.

In addition, data subjects should receive transparent information on the processing activities that are being carried out and their main features, including the retention period for collected data and the purposes of the processing. The information provided should be easily accessible and provided in clear and plain language.

It is important to adopt adequate security measures and confidentiality policies ensuring that personal data are not disclosed to unauthorised parties. Measures implemented to manage the current emergency and the underlying decision-making process should be appropriately documented.

3. Use of mobile location data

- **Can Member State governments use personal data related to individuals' mobile phones in their efforts to monitor, contain or mitigate the spread of COVID-19?**

In some Member States, governments envisage using mobile location data as a possible way to monitor, contain or mitigate the spread of COVID-19. This would imply, for instance, the possibility to geolocate individuals or to send public health messages to individuals in a specific area by phone or text message. **Public authorities should first seek to process location data in an anonymous way (ie. processing data aggregated in a way that individuals cannot be re-identified), which could enable generating reports on the concentration of mobile devices at a certain location ("cartography").**

Personal data protection rules do not apply to data which has been appropriately anonymised.

When it is not possible to only process anonymous data, the ePrivacy Directive **enables Member States to introduce legislative measures to safeguard public security (**Art. 15)**.**

If measures allowing for the processing of non-anonymised location data are introduced, a Member State is obliged to put in place **adequate safeguards**, such as providing individuals of electronic communication services the **right to a judicial remedy**.

The proportionality principle also applies. The least intrusive solutions should always be preferred, taking into account the specific purpose to be achieved. Invasive measures, such as the "tracking" of individuals (i.e. processing of historical non-anonymised location data) could be considered proportional under exceptional circumstances and depending on the concrete modalities of the processing. However, it should be subject to enhanced scrutiny and safeguards to ensure the respect of data protection principles (proportionality of the measure in terms of duration and scope, limited data retention and purpose limitation).

4. Employment

- **Can an employer require visitors or employees to provide specific health information in the context of COVID-19?**

The application of the principle of proportionality and data minimisation is particularly relevant here. The employer should only require health information to the extent that national law allows it.

- **Is an employer allowed to perform medical check-ups on employees?**

The answer relies on national laws relating to employment or health and safety. Employers should only access and process health data if their own legal obligations requires it.

- **Can an employer disclose that an employee is infected with COVID-19 to his colleagues or to externals?**

Employers should inform staff about COVID-19 cases and take protective measures, but should not communicate more information than necessary. In cases where it is necessary to reveal the name of the employee(s) who contracted the virus (e.g. in a preventive context) and the national law allows it, the concerned employees shall be informed in advance and their dignity and integrity shall be protected.

- **What information processed in the context of COVID-19 can be obtained by the employers?**

Employers may obtain personal information to fulfil their duties and to organise the work in line with national legislation.

For the European Data Protection Board

The Chair

(Andrea Jelinek)