The European Data Protection Board speaks out: Data Protection Measures in the Wake of COVID-19

Dr Emma Grech

4 April 2020

COVID-19 in a data-centric age

Since having first appeared in China during late 2019, COVID-19 – now classified by the World Health Organisation as a pandemic – has wreaked havoc across the globe. National responses to the contagion, while demonstrating a foremost commitment to the safeguarding of public health and the economy, have drawn considerable attention to the complementary notions of 'personal data' and 'data protection': this, of course, against a backdrop which has seen the surveillance of personal data by governments, public as well as private entities, take centre-stage in global efforts to "stop the spread".

The recognition of what, in today's technology and data-driven world, is an obvious premise – that, harnessed correctly, the processing of health (and other) data could constitute an effective tool to combat COVID-19 – begs the question: will the pre-contagion data protection law regime continue to be applied unchanged, possibly hindering the manner in which personal data may be 'exploited' by countries to fight the disease, or will today's dire state of affairs punch holes through the General Data Protection Regulation (EU 2016/679) (the "GDPR"): all for the 'greater good'?

The debate abounds especially as more jurisdictions across the world consider managing the pandemic through the use of software apps that could arguably lead to invasive privacy implications (for example, a 'track-and-trace' mobile application which would alert users if someone they have been in contact with tests positive for COVID-19).

image: Freepik.com

The EDPB's Guidance

In cognisance of this unprecedented situation, and with data protection authorities across Europe adopting differing measures, the European Data Protection Board (the "EDPB") published formal guidance (the "Statement") on the matter on 20 March 2020.

Therein, the EDPB emphasises that the GDPR should not stand in the way of the various COVID-19 measures being implemented by governments on the local plane, provided, however,that these are necessary, proportionate and consistent with the safeguards being imposed by the relevant national frameworks. The Statement essentially confirms that data controllers and data processors must, irrespective of the challenges faced in navigating the current crisis, continue to ensure that personal data are adequately protected.

To this end, the EDPB has put forward various considerations that ought to be taken onboard by entities to ensure that, during this crucial time, personal data are collected, stored and transmitted in a lawful manner.

Lawfulness of processing

The Statement confirms that the GDPR does allow entities to process personal data during a pandemic, in accordance with national law and the conditions set out therein, and – notably – without necessarily having to procure the consent of the data subject concerned. The EDPB proceeds to earmark the relevant legal bases under the GDPR which are pertinent to the collection of personal data in the COVID-19 scenario:

a. Processing that is necessary for reasons of substantial public interest in the area of public health– Article 9(2)(i) GDPR;

b. Processing that is necessary for compliance with a legal obligation – Articles 6(1)(c) and 9(2)(b) GDPR; and

c. Processing that is necessary to protect the vital interests of the data subject – Articles 6(1)(d) and 9(2)(c) GDPR. On this point, it is noteworthy that Recital 46 GDPR expressly refers to the control of an epidemic.

Principles relating to personal data processing

The Statement recalls that processing should only be carried out in accordance with the GDPR's data protection principles (Article 5(1) GDPR). Personal data should only be processed for 'specified and explicit' purposes, and only if such is necessary to attain the objectives intended. Moreover, data controllers – such as employers – should provide accessible and clear information to their data subjects – such as employees – in respect of the processing activities they are carrying out, as well as information regarding the purpose of the processing and the data retention period.

The message is clear: COVID-19 notwithstanding, individuals must be kept informed and transparent data processing measures adopted by all entities processing personal data.

Finally, the EDPB urges organisations to implement appropriate security procedures and put in place confidentiality policies to ascertain that personal data are not disclosed to unauthorised third parties. Measures adopted to manage the ongoing emergency, as well as any underlying decision-making processes in this regard, should be documented and logged.

Location data

Some EU member states may opt to use mobile location data in an attempt to closely monitor and mitigate the contagion. The EDPB advises that public authorities firstly look to anonymise location data – through, for example, data aggregation – as this would still grant visibility of the concentration of mobile devices in a particular location.

The Statement also recognises that, where it is not possible to anonymise location data, the so-called e-Privacy Directive (2002/58/EC, as amended) enables the introduction of measures at a national level to preserve public security (Article 15 E-Privacy Directive).

That said, any such measures must be proportionate, necessary and accompanied by adequate safeguards, such as the provision – to recipients of e-communication services – of the right to judicial redress. Where more aggressive measures are opted for, such as the 'tracking' of individuals through the processing of non-anonymised data, such should be subject to enhanced security measures and executed in strict adherence with the GDPR's data processing principles.

Employment context

The Statement clarifies that, provided that steps are taken internally to 'minimise' the amount of information collected – and this in accordance with the principle of 'data minimisation', the measures adopted are proportionate, and any applicable national rules are abided by, employers are permitted to process their employees' personal data – inclusive of health data – in order to prevent further contagion.

The EDPB also explains that while employers ought to inform members of their workforce if anyone has contracted COVID-19, they may not, however, divulge more information than is absolutely necessary to communicate the message

Where it becomes vital, for instance, for preventive or security purposes, to reveal the name of the employee that has been taken ill, and where national law allows it, the concerned employee is to be notified in advance. In such cases, and in its Statement, the EDPB makes it understandably incumbent upon the employer to protect the 'dignity and integrity' of the relevant data subject.

The IDPC's stance

On 20 March 2020, and following the publication of the EDPB's guidance, the Maltese Information and Data Protection Commissioner (the "IDPC") issued a statement regarding the processing of personal data in the context of COVID-19.

Therein, the IDPC encouraged entities to comply with the instructions provided by the public health authorities to mitigate the spread of the novel coronavirus. The IDPC emphasised the importance of implementing secure processing operations in order to achieve a desirable and just balance between the rights of the data subject on the one hand, and the need to process health data on the other.

Way forward

Given the current state of flux, organisations would do well to continue keeping tabs of guidance published at both a European level and at a national level by the relevant data protection authority situated in the jurisdictions in which they have a presence and in which they provide services.

GDPR violations could result in fines of up to the higher of €20M or, in the case of an undertaking, 4% of the total worldwide annual turnover of the preceding financial year. In addition, businesses are reminded that their data processing activities may not only be subject to inspections by the IDPC, but, depending on the nature of their activities, could be exposed to the scrutiny of data protection authorities situated abroad.

For information on how we may provide assistance on a data protection front, please contact Dr Emma Grech, Partner – emma.grech@thecitylegal.com

A: CITY LEGAL, Britannia House, Level 1, Old Bakery Street, Valletta, VLT1450, MALTA

E: mail@thecitylegal.com
W: www.thecitylegal.com
T: +356 2744 1120/1