EU Data Protection: COVID-19

The world is facing unprecedented challenges in its fight to contain Coronavirus (COVID-19). Various countries are in lockdown and emergency measures being implemented to contain the pandemic, with European countries currently at the epicentre of the outbreak.

Organisations are looking to adopt measures that support business continuity, whilst appropriately protecting the health and safety of workers, customers etc and complying with wider public health initiatives. The pace of response is fast moving, as the impact of the pandemic spreads quickly.

Application of the GDPR

As organisations implement emergency measures, it is important to be aware of the privacy implications of any steps being taken. In the EU, any measures which involve processing of personal data are likely to give rise to data protection compliance issues that will need to be managed consistent with the General Data Protection Regulation (GDPR).

The following are examples of some common measures being adopted by organisations which will give rise to processing of personal data and (in many cases) information about an individual's state of health which is subject to additional regulation as 'special category personal data' under the GDPR

- dealing with members of the workforce who are suffering from COVID-19, or who may be at risk, or who may have vulnerable family members
- tracing people who have been in contact with someone who has tested positive for COVID-19, or may otherwise be at high risk
- asking staff to complete questionnaires asking about potential exposure to the virus, or underlying health conditions or vulnerabilities which may present enhanced risks
- carrying out temperature checks on entry to sites
- sharing information with public health authorities

It is important to understand that the GDPR applies to these and similar response activities and there is no general waiver for compliance because we are dealing with a public health emergency. Compliance officers should bear this in mind and ensure that where measures are being adopted the usual principles are followed

to ensure processing is fair, lawful and transparent, necessary and proportionate with minimal levels of data captured for the required purposes and due confidentiality and retention controls applied.

Lawful conditions for processing data

In many cases, a key question will be what lawful basis applies under Article 6 of the GDPR and (in the case of health data being processed) Article 9. The most relevant Article 6 grounds are likely to be:

- "vital interests": the processing is necessary in order to protect the vital interests of the data subject or of another natural person.
- "legitimate interests": the processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data; or

Where processing involves health data, relevant Article 9 grounds include the following (noting that explicit consent is generally not going to be valid in respect of employees) :

- "preventative and occupational medicine": the processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law (Art 9(2)(h))
- "public health" the processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health … on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy (Art 9(2)(i))
- "employment law" the processing is necessary for the purposes of carrying out rights of the controller or data subject in the field of employment… insofar as it is authorised by Union or Member State law. (Art 9(2)(b))

As the italicised text above notes, this aspect of the GDPR is devolved to Member States with limited EU level harmonisation. This means local privacy and employment laws will need to be checked to understand the extent to which specific measures may be validly adopted on a per country basis when processing health data.

Response from data protection Supervisory Authorities

Regulators are aware of the challenges in this area and the risk that GDPR inadvertently prevents organisations taking necessary and appropriate measure to protect individuals from the pandemic. Over the last week we have seen almost all EU regulators issue guidance on this issue. The guidance is not consistent. The general theme is to explain that GDPR standards still apply throughout the pandemic and note the key provisions that need to be addressed encouraging organisations to be thoughtful about collecting excessive data and ensure health data in particular are not collected unless a special condition can be met. Most recognise the enhanced pressures that the pandemic brings and in some cases indicate that any shortfalls in compliance during the current period will be considered appropriately when considering enforcement. This may give some assurance to risk based decisions that are inevitably going to be made.

Critically some regulators have set out quite limited interpretations of the GDPR for key activities which we know are taking place routinely – for example stating that measures such as thermal checking and medical questionnaires should be reserved for public health authorities only, or must be conducted under the direct supervision of a health professional. In some cases, this guidance is being superseded by emergency legislation which we are seeing introduced which includes specific legal gateways relaxing these controls through further derogations to the Article 9 conditions.

Key takeaways

We recommend you take the following key steps when considering privacy risk associated any additional COVID-19 processing activities:

1. Ensure that measures implemented are consistent with current (and rapidly evolving) public health advice. This advice will inform what is necessary / proportionate under GDPR.
2. Limit the nature and volume of additional personal data processing activity to that absolutely necessary to carry out the relevant response measure. Wherever possible avoid processing specific health related information which can be linked back to an individual.
3. Ensure measures are strictly time limited to dealing with the current pandemic and curtailed once no longer necessary.
4. Ideally have all additional measures supervised and signed off by a health care professional / occupational health professional, in particular if health data are being processed.
5. Display a notice to explain what data is being collected, by whom and for what purposes and (as appropriate) update privacy policies.
6. Maintain a record of the lawful basis for processing.
7. Comply with the other relevant GDPR principles on retention, security etc.
8. Record the decision making in a data protection impact assessment.
9. When dealing with workforce data and related decisions, also consider compliance with employment laws and understand the impact on workforce rights, pay etc.

Regulatory Updates

The DLA Piper privacy team are closely monitoring the regulatory position across the world. We are sharing information within our team to keep up to date with latest global developments which are evolving on a daily basis.

For further information and support, please get in touch with your usual DLA Piper contact.

By: Andrew Dyson & Patrick Van Eecke

The article originally appeared here.