Covid-19 and the GDPR
Important Information and Considerations

This Edition 16th March 2020

Managing the COVID-19 outbreak and stopping its spread is now a global challenge. In addition to the significant health and medical responses underway around the world, governments and public health officials are focused on how to monitor, understand and prevent the spread of the virus. Data protection and privacy laws, including the EU General Data Protection Regulation and the UK's Data Protection Act 2018, are informing these responses.

One major response to limiting the spread of infection is contact tracing, which is the practice of identifying and monitoring anyone who may have come into contact with an infected person. Employers, governments and educational institutions are also imposing travel restrictions, instituting self-quarantine policies, limiting visitors, and considering whether to require medical examinations. These responses necessarily involve obtaining and potentially sharing personal information, including data about an individual's health, travel, personal contacts, and employment. For example, in the United States., the Centers for Disease Control and Prevention has asked airlines for the name, date of birth, address, phone number and email address for passengers on certain flights.

EU countries (including the UK) collecting personal data as part of their COVID-19 response will be required to comply with the GDPR (as well as their own laws). For example, Italy's data protection authority, the Garante, adopted a decree addressing the intersection between the GDPR and COVID-19, the need for processing special categories of personal data, and how some data protection rights could be suspended to combat the virus. The Garante has issued further guidance prohibiting "do-it yourself" data collection. DPAs in France and Ireland have likewise taken positions on the handling of personal data in the context of responding to COVID-19.

The GDPR also addresses public health crises specifically and includes provisions relating to the processing of personal data.

PART 1

The UK Information Commissioners Office Satements
Data Protection And Coronavirus: What You Need To Know

The ICO recognises the unprecedented challenges we are all facing during the Coronavirus (COVID-19) pandemic. We know you might need to share information quickly or adapt the way

you work. Data protection will not stop you doing that. It's about being proportionate - if something feels excessive from the public's point of view, then it probably is.

Question 1

During the pandemic, we are worried that our data protection practices might not meet our usual standard or our response to information rights requests will be longer. Will the ICO take regulatory action against us?

No. We understand that resources, whether they are finances or people, might be diverted away from usual compliance or information governance work. We won't penalise organisations that we know need to prioritise other areas or adapt their usual approach during this extraordinary period.

We can't extend statutory timescales, but we will tell people through our own communications channels that they may experience understandable delays when making information rights requests during the pandemic.

Question 2

More (if not all) of our staff will be homeworking during the pandemic. What kind of security measures should my organisation have in place for homeworking during this period?

Data protection is not a barrier to increased and different types of homeworking. During the pandemic, staff may work from home more frequently than usual and they can use their own device or communications equipment. Data protection law doesn't prevent that, but you'll need to consider the same kinds of measures for homeworking that you'd use in normal circumstances.

Question 3

Can I tell my staff that a colleague may have potentially contracted COVID-19?

Yes. You should keep staff informed about cases in your organisation. Remember, you probably don't need to name individuals and you shouldn't provide more information than necessary. You have an obligation to ensure the health and safety of your employees, as well as a duty of care. Data protection doesn't prevent you doing this.

Question 4

Can I collect health data in relation to COVID-19 about employees or from visitors to my organisation? What about health information ahead of a conference, or an event?

You have an obligation to protect your employees' health, but that doesn't necessarily mean you need to gather lots of information about them. It's reasonable to ask people to tell you if they have visited a particular country, or are experiencing COVID-19 symptoms.

You could ask visitors to consider government advice before they decide to come. And you could advise staff to call 111 if they are experiencing symptoms or have visited particular countries. This approach should help you to minimise the information you need to collect.

If that's not enough and you still need to collect specific health data, don't collect more than you

need and ensure that any information collected is treated with the appropriate safeguards.

Question 5

Can I share employees' health information to authorities for public health purposes?

Yes. It's unlikely your organisation will have to share information with authorities about specific individuals, but if it is necessary then data protection law won't stop you from doing so.

PART 2

Three Rights (Articles) In Particular Are Relevant To Our / Your Work In School's and Academies

These Are :

Processing Without Consent - The Right to Erasure - Processing of Special Categories

Article 6 — Processing Without Consent

The GDPR's Article 6 provides that the processing of personal data without consent is lawful where it is necessary for compliance with a legal obligation to which the controller is subject, to protect the vital interests of the data subject or of another natural person, or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. It also states that "[s]ome types of processing may serve both important grounds of public interest and the vital interests of the data subject as for instance when processing is necessary for humanitarian purposes, including for monitoring epidemics and their spread or in situations of humanitarian emergencies, in particular in situations of natural and man-made disasters." Therefore, in this regard, processing personal data "should also be regarded to be lawful where it is necessary to protect an interest which is essential for the life of the data subject or that of another natural person." It also suggests that the "vital interest" exception should be construed narrowly, stating processing personal data based upon the vital interest of another natural person "should in principle take place only where the processing cannot be manifestly based on another legal basis."

Article 6 does impose some limitations on these exceptions, requiring the basis for processing personal data under the public interest exception or to comply with a controller's legal obligation be an EU or member state law and that this law "meet an objective of public interest and be proportionate to the legitimate aim pursued." Member States also may adopt more specific provisions with regard to processing for compliance with a legal obligation or for performing a task in the public interest, including to ensure such processing is lawful and fair.

In addition, the principles in Article 5 relating to the processing of personal data, including transparency, would still apply, except where restricted by member state law for reasons of national security, public security, to protect the rights and freedoms of others, or for other similar exemptions outlined, each require a "necessary and proportionate" test.

Article 9 — Processing Special Categories Of Data

The GDPR's Article 9, which prohibits processing of special categories of personal data (including biometric and health data) without explicit consent, also has similar exceptions, including where processing is necessary:

1. "to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;"
2. "for reasons of substantial public interest;"
3. "for the purposes of preventive or occupational medicine. . . medical diagnosis. . . [or] the provision of health or social care or treatment;" and
4. "for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health."

Additionally, it acknowledges the need for processing special categories of personal data for "the prevention or control of communicable diseases and other serious threats to health" and emphasises that such data should be processed for health related purposes "only where necessary to achieve those purposes for the benefit of natural persons and society as a whole," with EU or member state law providing "specific and suitable measures" to protect the data. Furthermore, it recognises processing special categories of personal data without consent may be necessary for public health reasons but makes clear such processing should not result in the data being processed for other purposes by third parties, such as employers or insurance companies.

Article 17 — Right To Erasure

It is worth noting the provisions in Article 17 regarding the right to erasure of personal data do not apply to the extent processing is necessary "for reasons of public interest in the area of public health." The provisions referenced above make clear the authors of the GDPR anticipated the situation now unfolding, as authorities grapple with how best to safeguard the health, well-being and personal data of individuals across the EU and around the globe.

Produced By Illuminate Learning For DPO Contracted Schools

Illuminate Education Services UK Ltd
E : contact@illuminatelearning.org
W : illuminatelearning.org
T : 01704 288202