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.

And the ICO is here to help – please see below for answers to the questions we're being asked. If you need more help, call us on 0303 123 1113.

We have also produced specific advice for health and social care organisations during the coronavirus pandemic, along with guidance for employers conducting workplace testing and for businesses collecting personal data for contact tracing. There's also more advice on our dedicated Data Protection and Coronavirus hub page.

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.

The ICO has published a document setting out our regulatory approach during the coronavirus pandemic.

More 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 security measures for homeworking that you'd use in normal circumstances.

Our Working from Home guidance provides more detailed advice.

I have set up a community group in my neighbourhood to help vulnerable and self-isolating people. What are my data protection obligations?

Data protection won't stop you from helping people, but there are certain things you need to take into account when handling people's information. We have published a blog for community groups on what they need to know about data protection.

As a community group and not-for-profit organisation, you are not required to pay the ICO's registration fee. However, it's still important that you follow data protection guidance when handling people's information.

How should I tell people about how we're processing personal data during the pandemic?

Where possible, organisations should have clear and accessible privacy information in place before processing begins. However, we recognise that in this exceptional period, this may not always be possible.

Organisations should ensure that privacy notices are in place and updated as soon as reasonably practical. More details of what they should include can be found on our website, where there is also a simplified version that may be helpful to organisations.

The sort of information that they ought to include might be (but isn't limited to):

- An organisation's name and contact details (email and telephone number),
- The data held and the reasons why,
- Where this data was obtained,
- The length of time it will be retained for, and
- How people can request it be erased.

Where possible, organisations should make this information as accessible as possible, consider the different circumstances and factors that will impact upon this, and communicate accordingly.

I'm worried we're more open to a personal data breach because of adaptations we've made during the pandemic. What should I do?

Many organisations have had to adapt to the evolving pandemic at speed, for example, arranging working from home quickly and using new IT solutions, which in turn may have led to policies procedures not being strictly followed.

We have seen several breaches involving human error such as using CC instead of BCC on emails and sending personal data to incorrect recipients so it may be worth reminding your staff to check before sending emails.

Our Working from Home guidance can help your organisation remain compliant with data protection laws.

How can I show that our approach to processing during the pandemic is compliant with data protection law?

To show that your processing of data is compliant, you will need to use the accountability principle. It makes you responsible for complying with the GDPR and says that you must be able to demonstrate your compliance such as additional recording keeping requirements when processing sensitive data. One way of demonstrating accountability is through a data protection impact assessment (DPIA).

If your organisation is going to process health information, then you should conduct a DPIA focussing on the new areas of risk.

This DPIA should set out:

- the activity being proposed;
- the data protection risks;
- whether the proposed activity is necessary and proportionate;
- the mitigating actions that can be put in place to counter the risks; and
- a plan or confirmation that mitigation has been effective.

DPIAs are designed to be flexible, as appropriate to the context. We have a template organisations can use to help them focus on the minimum requirements. One important point is that the initial DPIA should be regularly reviewed and updated. This is especially important in a fast-moving crisis situation, as new risks and benefits emerge.