Browne Jacobson

# Data protection and Coronavirus

The ICO has recently released updated guidance for businesses who are grappling with concerns around data protection compliance during the ongoing Covid-19 (Coronavirus) pandemic

08 April 2020

**Please note: the information contained in our legal updates are correct as of the original date of publication**

The ICO has recently released updated guidance for businesses who are grappling with concerns around data protection compliance during the ongoing Covid-19 (Coronavirus) pandemic.

Businesses are facing challenges in two main areas: (1) compliantly collecting and sharing personal data relating to Coronavirus; and (2) data compliance issues due to staff working from home, or off due to illness. Whilst the first of these issues is specific to the pandemic, the data issues related to working from home in particular are likely to endure well beyond the end of the pandemic, so is causing some businesses to look again at their processes.

The key message from the Information Commissioner's Office (ICO) is to be proportionate in your approach – if something feels excessive from the public's point of view, then it probably is. The ICO reassures businesses that it is a "pragmatic and reasonable regulator, one that does not operate in isolation from matters of serious public concern". Data protection compliance should not stand in the way of you protecting the health of your staff and others, or the ability for you to run your business, but you must ensure that you adhere to the key principles of data minimisation and fairness to data subjects.

## 1. Collecting and sharing personal data related to Coronavirus

In order to protect the health of your staff and others at this time, you may need to collect and share more personal data than usual. For example, you may need to collect information about whether your staff, supplier staff, or visitors to your premises are experiencing symptoms of Coronavirus, or have come into contact with anyone experiencing symptoms of Coronavirus. You may also need to share some of that information internally with key decision makers, or third parties including your suppliers and clients. Here are some key steps you should take to ensure compliance.

- Only process personal data that is necessary and proportionate in the circumstances. For example, if you have been informed by an employee that they have Coronavirus, you may inform certain other employees that they have been in contact with someone who has Coronavirus, however it is unlikely to be necessary to share the name of the relevant individual.
- Ensure that you have a legal basis to process personal data (as required under Article 6 of the GDPR). Personal data is any information that identifies an individual such as names, contact details, job roles, and location data. You must ensure you have an applicable legal basis for each different purpose for which you are processing the data. For example, where you are processing personal data relating to employee sickness, the appropriate legal basis under Article 6 is likely to be that such processing is necessary for the performance of the employment contract.
- Ensure you have a condition for processing "special categories of personal data" (e.g. health data) (as required under Article 9 of the GDPR). There is a general prohibition on processing special categories of personal data unless one of the conditions in Article 9 applies. The most relevant conditions for these purposes are likely to be that the:

    1)*"processing is necessary for the purposes of carrying out or exercising specific rights of the controller or the data subject in the field of employment"*; or

2)*"processing is necessary in order 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".*

However, any processing will be subject to the principle of necessity (as set out above) – do not collect or share personal data unless strictly necessary for a particular purpose. For example, you may require health data from your team relating to requests for work from home kits. It is likely to be necessary to share that data with HR and the relevant person's line manager, although it is unlikely that that information would need to be shared with any other individuals.

- Ensure that any correspondence or documents containing personal data are kept secure. Keep any personal data (particularly sensitive data) on a secure drive with access restricted to only those who need to see the information. Consider password protecting documents where appropriate. The level of security required will depend on the sensitivity of the data in question - stricter measures should be in place for health data and other special categories of personal data, as these pose a higher risk.

## 2. Ongoing data protection compliance

With a large proportion of the UK workforce now working from home and many businesses' resources strained due to staff illness, complying with ongoing data protection obligations is likely to become more challenging. We have set out below some key areas of ongoing data protection compliance which may be affected.

- Responding to rights requests (including the right of subject access and the right to be forgotten). The statutory deadline to respond to such requests is one calendar month. Inevitably, with limited resources and key staff working from home, businesses may struggle to comply with those deadlines. The ICO has said, "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", which is comforting to controllers who will struggle to deal with rights requests because of these unprecedented challenges. However, you must still respond to and deal with rights requests as best you can given the circumstances, so that you can show that you have acted reasonably. Maintaining a dialogue with the data subject is key. If you are unable to comply within the statutory deadline, consider seeking to invoke the 2 month extension.
- Security concerns arising from staff working from home. Consider your current working from home and information security policies. Do these need to be updated in light of the current circumstances? Do you have adequate security measures in place to protect personal data (particularly special categories of personal data) that is processed by staff working from home? If it is necessary that staff have copies of personal data outside of their usual working environment (for instance on their own laptop), consider how this will be disposed of in a secure and timely manner. How will you ensure that meetings carried out by video conference are secure? What software will you permit people to use in your business and what controls are in place?
- Privacy notices. Do you need to update your privacy notices/policies to inform individuals of any new processing activities, or provide a short form notice in respect of specific processing activities? For example, you may not previously have collected health data about visitors to your premises. In those circumstances, it may be appropriate to draft a short paragraph setting out why you are collecting that data, and for how long it will be stored (referring out to your main privacy notice/ policy).
- Record of processing activities (ROPA). Do you need to update your ROPA to add any new purposes for processing personal data or new third party software providers?

Co-authored by Loren Hodgetts and Ella Greenwood

# Contact

Mark Hickson

Head of Business Development

onlineteaminbox@brownejacobson.com

+44 (0)370 270 6000

## Related expertise

Criminal compliance and regulatory

Data protection and privacy