Client Alert: Returning to Office Working - Health Testing and Data Protection

Date : June 8, 2021

We first published this alert in May 2020 and we're updating it from time to time with more questions and developments.

Introduction

As lockdown restrictions have changed in some countries, many companies have been dealing with partial returns to company premises or so-called hybrid working where employees work from company premises and at home. Obviously protecting employee health and safety is paramount, but what measures can organisations reasonably take to support their return to work efforts? And how do they ensure that data protection laws are complied with when more sensitive personal data, such as health data, is collected.

This article follows on from our previous FAQs on the data protection aspects of COVID-19 which includes links to guidance in more than 40 countries – www.bit.ly/gdprvirus. There are some data protection specific terms in this note which are explained at www.bit.ly/gdprwords. We refer to GDPR in this note and post-Brexit we're really referring to EU GDPR and the so-called UK GDPR in this context. You can find out more about UK GDPR here https://bit.ly/brexdpfaq.

What is the government guidance on safe working practices during the COVID-19 outbreak?

Governments in different countries have now issued guidance on returning to the workplace. For example, the UK Government's advice is now detailed and different depending on the place of work. Similar guidance has been issued in other countries although with some differences – for example guidance on the safe distance varies.

When can organisations process employee health data?

As a reminder, health data is special category data under GDPR Article 9, and requires one of a number of specific exemptions to be met in order for it to be lawfully processed. The main way to legitimise the handling of health data, which is likely to be relevant to workplace testing, is processing for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment (GDPR Article 9(2)(b) together with local law in some cases).

This is subject to a necessity test, which means the processing must be *necessary* to the relevant purpose being fulfilled – it is not enough that a specific way of processing might be convenient if other less data protection intrusive alternatives are available.

Some employers seem to be seeking to rely on a data subject's consent but in an employee / employer context consent could be problematical (essentially because of the inequality of bargaining power) and it can be withdrawn. As a result, consent will not always be the best solution unless you can provide a genuine alternative.

Ultimately, you will need to assess the relevant legal basis that best suits the specific back to work scenario you are facing on a case by case basis.

Some regulators have released specific guidance and in November 2020 two unnamed companies based in the Netherlands were ordered by the Dutch DPA (the Autoriteit Persoonsgegevens or AP) to change their policies regarding employee temperature checks. The AP carried out a random audit to see if businesses were meeting their GDPR obligations. The companies who failed the audit will apparently have a repeat audit as part of the AP's enforcement program.

It is also important to remember that health data could be widely defined. For example in a case in Austria in

November 2020, the Austrian DPA held that a restaurant in Vienna could not collect data via a QR code limited to name, phone number, email (which was optional) and table number. The restaurant said that it collected data "*to protect the life and health of our employees and our guests in connection with the occurrence of the Coronavirus and the COVID-19 pandemic*". The DPA said that whilst that did not qualify as health data in itself, in the context of COVID-19 contact tracing, the data contained information about the past, present and future physical or mental state of health of the diner. As a result effectively the Austrian DPA said that even this limited data should be treated as sensitive personal data under GDPR. The Austrian DPA also decided that consent could not be a valid basis for processing diners' data as it was not freely given. They based this on the fact that there were no acceptable alternative for the customer – if you wanted to eat a diner had to give them his details. They took into account the fact that there was no acceptable alternatives for the diner since all restaurants in Vienna were likely to have a similar tracking system in place.

As an example of the DPA guidance in this area in the UK the Information Commissioner's Office (ICO) has released guidance on workplace testing – there's a link to this guidance below. It is important to remember that for EU countries whilst GDPR sets out a basic framework local law can differ even within the EU. It is also important to stress that guidance from regulators is just that – we can expect to see litigation and the courts may not follow any guidance which has been issued by a regulator. For example an employee disadvantaged as a result of data processed relating to their health may well try litigation alleging that data processing was unlawful. Organisations need to gear up for the more frequent exercise of subject access requests under GDPR too. There is a special risk of exercise of GDPR rights from employees who have been furloughed or let go.

If you're using a third party or an app to help you make sure you've done proper due diligence on the provider too. As we said in our alert in March 2020 a number of start-ups are pitching solutions which may not be as good or as secure as they seem. If you are using a third party or app you will also need to look at your transparency obligations under GDPR too – that's likely to include disclosing who the provider is, where they will host data, what they will do with it and how long they will keep it for. You'll also need to check that the app doesn't collect more data than it needs to do the job – for example collecting data for advertising purposes will be very hard to justify.

The ICO's 12 June 2020 guidance suggests you start by asking 4 questions:

1. How will collecting extra personal information help keep your workplace safe?
2. Do you really need the information?
3. Will the test you're considering actually help you provide a safe environment?
4. Could you achieve the same result without collecting personal information?

Note that as concerns about the virus reduce some data protection authorities are changing their guidance – for example on 2 June 2020 the Latvian DPA revised its guidance to suggest that employers should no longer be collecting COVID-19 related data on an employee's health.

Can organisations require staff temperature checks?

Some jurisdictions (for example parts of Germany) ban temperature checks. In others temperature checks are only likely to be justified when all other reasonable less intrusive means have been exhausted and it is a proportionate response to the risk you are trying to address. For example, you would need to have already explored measures such as:

1. reducing activity times;
2. using screens or barriers to separate people from each other;
3. using back-to-back or side-to-side working whenever possible;
4. staggering arrival and departure times; and
5. reducing the number of people each person has contact with by using 'fixed teams', 'partnering' or 'work bubbles'.

Depending on the circumstances it could be that temperature checks would only be able to be used on staff who cannot feasibly work from home, where the nature of the work that they undertake means that being in close

proximity to others cannot be avoided and if one person is infected there is a high risk of them infecting many more people. A DPIA will help you make these decisions. Also look at the technology to be used – a Spanish case in May suggests that a temperature scanner which does not collect personal data but simply gives a 'high' or 'normal' result in itself may be lawful.

This issue of proportionality was also explored in the slightly different context of biometric fingerprinting by the AP in The Netherlands, which fined a company €725,000 in April 2020 for unlawfully processing fingerprints of its employees for attendance and time registration purposes.

What about other more detailed COVID-19 diagnostic testing?

This might be an area where guidance differs between countries and so you may need to take a look at the relevant law and guidance in those countries where you have operations.

The Italian DPA has said that Italian companies cannot directly perform COVID-19 diagnostic tests on employees. However, an organisation can ask its employees to carry out those tests if ordered by a competent doctor or healthcare professional. In addition, the processing of employee diagnostic data or family history to assess return to work can only be undertaken by competent healthcare professionals and not by the companies themselves.

In the UK the ICO has not been as prescriptive but it makes sense that diagnostic tests should only be undertaken by medically trained personnel and processed in laboratories with industry-approved testing standards. The ICO has also said that, where staff provide test results voluntarily, those results would need to be kept secure and you would need to consider any duty of confidentiality owed to those individuals who have provided test results.

Can organisations require that staff disclose if they are from a vulnerable / high risk group?

An employer would generally be justified in requesting health data relating to a staff member having a condition that puts them at greater risk of becoming seriously ill in order to assess if that person can safely return to work. However, it may be reasonable to ask employees to confirm if they have any of certain listed underlying conditions, rather than making them specify which one.

The organisation may already hold some information about employees' serious underlying health conditions, for example, in case they require special adjustments or something happens to them at work and they need medical treatment or for company-run health insurance schemes. The question then becomes whether use of health data that the company already holds for those purposes can also be used for purposes related to their return to work or return to the office. In line with the "purpose limitation principle", this will require an assessment as to whether further processing is *compatible* with the original purpose for which the data was collected. If not, it may be necessary to obtain consent to use the data for any further purposes.

You'll also need to be sensitive about how you collect this data. For example if you are using technology designed to assess likely risk at the entrance to a building (such as COVID arches or Rokid detection devices) you will need to make sure that employees are not forced to share their personal data where they can be overheard by co-workers and others in a queue to enter the building.

Can organisations require staff to participate in a government track and trace program?

In our view, it is unlikely to be reasonable for organisations to force staff to participate in any government track and trace programme (which itself will be voluntary), nor could staff be forced to share track and trace app data with their employer. Whilst organisations could encourage staff to participate, this would need to be entirely their choice and they should not be penalised if they do not participate. Any communications about this would need to be carefully worded.

Are there any data security issues?

Possibly. The issues you face are likely to depend on how you've been dealing with working from home. For

employees who have fixed computers at work its wise to remember that they may have missed some software patch cycles if they have been switched off during the pandemic. Criminals are likely to exploit known vulnerabilities – our alert here looks at some of the issues with increased cybercrime during the pandemic - https://bit.ly/cvransom. It could also be wise to check your vulnerabilities if employees are returning to work with devices that have been off the network for a long period of time – in some cases more than a year. It might not have been 'business as usual' for some devices too, especially if you have a BYOD policy, as devices may have been used for home schooling, streaming or Zoom cocktails.

What about mixed home and office working?

Many organisations are looking at a gradual return to work with some employees staying at home. It's important to remember that for those employees still at home you'll still need to make sure that personal data continues to be protected, employees are told how to avoid phishing attacks etc. There's some guidance on that in our earlier alert here www.bit.ly/gdprvirus. Now might be a good time to review any earlier assessment of risk to make sure your risk assessment is still valid and to see if extra measures are justified given that working from home for some (especially those who are vulnerable) is likely to continue for much longer than some may have originally envisaged. You should also be careful about monitoring – for example there are particular issues with O365 productivity tools.

Remember the risks with hard copy data too. If employees are carrying hard copy data into and out of the office make sure you have a system in place to log data out and to log it back in. A recent case in Poland has reminded us that DPAs will also take action if hard copy data is lost - https://bit.ly/polehard.

What about hygiene declarations?

Some organisations are requiring employees to sign hygiene declarations promising that they will wash their hands regularly and adopt additional hygiene measures. Again organisations will need to exercise caution when implementing this type of system and will need to pay attention to the tone of these messages and the system they plan to use. A DPIA is likely to be required. If the data is held electronically they will need to look at where the data is held to avoid data transfer issues. In some cases prior consultation or notification to a works council may also be required. Care must also be taken not to unintentionally vary employment contacts especially at a time of extra sensitivity for employees.

What about helpline calls?

We are already seeing anecdotal evidence that helpline calls are rising with employees raising concern about the behaviour of others in the workplace. Some of these concerns are likely to be genuine and are likely to require investigation. We have written about the heightened corruption risks business currently face for example here https://bit.ly/covbribe. Organisations will need to be careful however about employees raising more trivial concerns. Some jurisdictions (including France and Germany) require helplines to be focused on key areas of possible harm. Employees with more minor concerns should be encouraged to raise concerns with their line manager rather than a whistleblower line. Remember that this is a time when whistleblower laws in the EU are also undergoing change (see https://bit.ly/euwhistle).

What steps should organisations take when getting staff back to office or hybrid working?

Organisations should consider the following:

1. **Carry out a Data Protection Impact Assessment (DPIA)** – given that processing health data has higher privacy risks associated with it, we would recommend getting expert legal advice. Cordery has worked with clients on many DPIAs and can help you through the process.
2. **Decide on your legal basis for processing** – ensure that processing is necessary and proportionate to the purposes you are seeking to fulfil, and be careful about using consent.
3. **Update privacy notices <u>before</u> testing starts** – these should include clear and transparent information about what personal data is required, what it will be used for, any recipients that it will be shared with and

how long the data will be retained for.

4. **Do not collect unnecessary or excessive information from people**.
5. **Check and maintain health data for accuracy** – ensure that test results are dated and deleted as soon as these are no longer valid or are superseded by a more recent test result.
6. **Make security of employee health data a top priority**.
7. **Set up systems and processes** - to be able to respond expeditiously to data subject requests in relation to such health data.

Resources

There is more information about this and other data protection topics in Cordery's GDPR Navigator subscription service. GDPR Navigator includes short films, straightforward guidance, checklists and regular conference calls to help you comply. More details are at www.bit.ly/gdprnav.

The UK Government guidance is here - https://bit.ly/3eJxywZ and there is guidance from the ICO here https://bit.ly/3e6uoDN

Details of the Dutch case on biometric data are here https://bit.ly/3eIxbTx and details of the Austrian restaurant case are here http://bit.ly/37tJgee.

The Latvian guidance is here https://bit.ly/3ejihU9

There are links to guidance in more than 40 countries in our original alert here www.bit.ly/gdprvirus

BSI has published draft safe working guidance which might be useful - https://bit.ly/36WzjUZ

For more information please contact Katherine Eyres or Jonathan Armstrong who are lawyers with Cordery in London where their focus is on compliance issues.

Office: +44 (0)207 075 1784

jonathan.armstrong