Local Connections. Global Influence.

COVID-19

Key Privacy Concerns Raised by “Back-to-Work” COVID-19 Safety Measures

UK – 20 May 2020

squirepattonboggs.com

On 10 May 2020, Prime Minister Boris Johnson informed businesses in England that, as part of the Government's three-phase strategy for lifting the Coronavirus lockdown, employees that cannot work from home can, and should return to work from Wednesday 13 May 2020.

Although not all industries are able to re-open during this first phase of the eased restrictions, a clear roadmap has been established, which aims for most businesses to resume by this summer, unless the virus begins to escalate once again.

In order for employers to comply with their health and safety obligations and Government guidance, they can only allow employees to return to work if it is safe for them to do so. This will require a workplace risk assessment and the implementation of measures that are aimed at combatting the spread of the virus amongst the workforce and those they come into contact with. This may include the use of personal protective equipment, restructuring the office or site to enable social distancing and providing additional hand-washing facilities.

However, it may also include measures such as the use of temperature testing or thermal imaging cameras, rolling out a 'track and trace' app to employees or testing employees for the virus, all of which raise data privacy issues as they involve the processing of 'personal data', which is governed by strict data protection laws.

These laws are not intended to act as a barrier against taking measures that may be highly effective as part of a strategy to fight the virus. However, businesses do need to ensure that their use of personal data is proportionate and limited to what is necessary to comply with their health and safety obligations, in order to minimise the risk of adverse consequences, such as regulatory enforcement action and claims under data protection laws.

This note aims to provide practical advice on some of the key data protection compliance measures that should be factored into a business's post-lockdown "back-to-work"plan, together with a quick-reference checklist:

1. Testing employees: Thermal cameras & temperature testing

Many businesses have already started to carry-out temperature testing at their sites or offices, or plan to do so. This may include manual temperature testing, or the use of thermal-imaging cameras.

Before implementing any form of temperature testing, the business needs to assess whether this is a necessary and proportionate measure to ensure the health and safety of its workforce and others. One potential issue here is whether temperature testing is an effective method of identifying those with COVID-19? A raised temperature does not necessarily mean that an individual has the virus, which could make it difficult for a business to assert that this is a necessary and proportionate measure to combat its spread.

Nevertheless, given the severity of the COVID-19 pandemic, businesses will understandably want to do everything they can to ensure the safety of their employees and given that a raised temperature is one of the key indicators of the virus, temperature checking will be viewed by many businesses as a key part of a wider strategy to fight the virus.

Businesses are advised to document their assessment of whether temperature testing is a necessary and proportionate measure to comply with their health and safety obligations (in conjunction with other planned measures) and how they will comply with their data protection obligations in relation to the personal data processed as a result. This includes ensuring that the scope of personal data collected and its use, disclosure and retention are strictly limited to what is necessary to comply with health and safety obligations ("data minimisation").

Businesses need to be fully transparent with employees and visitors about their use of any personal data collected during temperature testing, including providing a GDPR-compliant privacy notice to supplement their employee and website (site visitor) privacy notices.

If a business opts to use thermal-imaging cameras, this may constitute employee monitoring and surveillance activity, which is considered particularly intrusive and may require a Data Protection Impact Assessment to be conducted. The business needs to be able to demonstrate that the use of these cameras is necessary to comply with health and safety obligations and specifically that less intrusive measures are unlikely to be sufficiently effective.

Clear signs will need to be erected at the site of the cameras, alerting employees to their presence and purpose. The signs should include a link to a GDPR-compliant privacy notice.

It is important to keep an open dialogue with employees, which clearly identifies that temperature testing and the other measures taken by the business are critical to get people back to work safely. If the workforce are on-board from the outset, this will substantially reduce the risk of complaints and the resulting potential enforcement action or claims.

2. COVID-19 testing

Some businesses are already carrying out, or plan to carry out COVID-19 testing of their employees (and in some cases family members).

Handling an employee's COVID-19 test result will involve the processing of health data (as may handling the result of a temperature check). Health data is categorised as 'Special Category Data' under UK data protection laws, which is subject to stronger controls, due the increased risks associated with misuse of it.

As a result, businesses need to be very confident that the use of this data is necessary and proportionate in order for them to comply with their health and safety obligations. A Data Protection Impact Assessment will need to be carried out to document this assessment and the individuals tested will need to be fully informed about how their data will be used.

It is particularly important to adhere to data minimisation and not to collect excessive information. For example, collection of the test results may be necessary, but not any information about underlying health conditions. It is important to record the date of the test for data accuracy purposes, as a person's health status will change over time.

Robust data security and access restrictions should be in place to protect the data. Health data should be handled, wherever possible, by suitably qualified health professionals and access to medical information by managers should be strictly limited to what is necessary for their managerial responsibilities.

Businesses should avoid relying on employee consents as a lawful basis to process this data, as they are unlikely to be valid, due to the perceived imbalance of power between employees and their employers.

3. Track & Trace apps

NHSX Contract-Tracing App

The new NHSX contact-tracing app is viewed by many as a key tool to enable the lifting of the lockdown, whilst continuing to combat the spread of the virus. Many employers may be keen for their employees to download and use it when it is rolled-out in the UK, in order to help them to combat the spread of the virus within their own organisation. Use of the NHSX contact-tracing app is likely to be voluntary in the general population. However, an instruction by an employer for their employees to use it may well be considered to be a reasonable management instruction from an employment law perspective.

Employers will want to be promptly informed if an employee receives an alert on the app to indicate that they have recently been in contact with someone who is infected with the virus. Restricted use of this information is likely to comply with data protection laws, as it will be information that the employer needs to help it to limit the spread of the virus within its business and to make arrangements to enable the employee to self-isolate, thereby complying with its obligations relating to employment. However, a Data Protection Impact Assessment may be required to document this.

As when dealing with COVID-19 test results, strict data minimisation and robust security measures will be required to protect the data and businesses will need to be fully transparent with employees about how this data will be used.

Using Bespoke 'Track & Trace' Apps

A number of businesses have already implemented their own apps to track and trace contacts between employees and recent statistics suggest that many others may wish to follow.

Employers should be mindful of the fact that when they implement one of these apps, they will be the controller of any personal data collected and as a result, they will need to ensure that the app complies with the privacy by design and default obligation under UK data protection laws and that personal data is processed lawfully, fairly and transparently.

This must include strictly limiting the scope of the personal data collected and the use of, access to and retention of it. For example, the NHSX app is designed to match devices via anonymous Bluetooth identifiers, rather than using GPS, which uses location data and that is considered far more intrusive. It also limits the amount of personal data that is stored and can be accessed centrally, enabling the storage of some data on the device itself. In addition, access to this data will be limited to the NHS, which, as a public health authority, has a strong legitimate need to use this data to fight the pandemic.

Employers should carry out careful due diligence before rolling a track and trace app out to their employees, including carrying out a Data Protection Impact Assessment (or ensuring that a DPIA carried out by the app developer demonstrates compliance with data protection laws). It will be important for an employer to justify why use of their app is a necessary and proportionate measure to supplement the NHSX app and to enable them to comply with their health and safety obligations.

Employers will need to ensure that GDPR-compliant privacy notice information is provided to all those using the app. This may involve using a layered approach, which includes the provision of information up-front before use of the app, in addition to further information during use, such as just-in-time notices.

Other key considerations include:

- Building-in appropriate privacy protections and default settings;
- Ensuring strong data security measures are in place;
- Collecting the minimum data necessary to achieve your specified purpose; and
- Considering appropriate data retention periods and implementing a framework for the dismantling of the app once the COVID-19 crisis has ended.

✓ 4. What can employers tell employees about cases of the virus in the workplace?

In order to protect the health and safety of the workforce, employers may wish to tell staff if there has been a (suspected or confirmed) case of COVID-19 in the workplace. The data protection regulator in the UK, the Information Commissioner's Office ("ICO"), states that employers should let staff know about infections, but that employees should not be named, if possible, and the information divulged should be kept to a minimum.

✓ 5. How to use health data provided by employees

In many cases, employees will voluntarily inform their employer that they, or a member of their household, have tested positive for COVID-19. Employers will have a lawful basis to process this special category data for the restricted purposes of taking the necessary measures to combat the spread of the virus and for workforce planning, subject to compliance with data protection obligations, as discussed above.

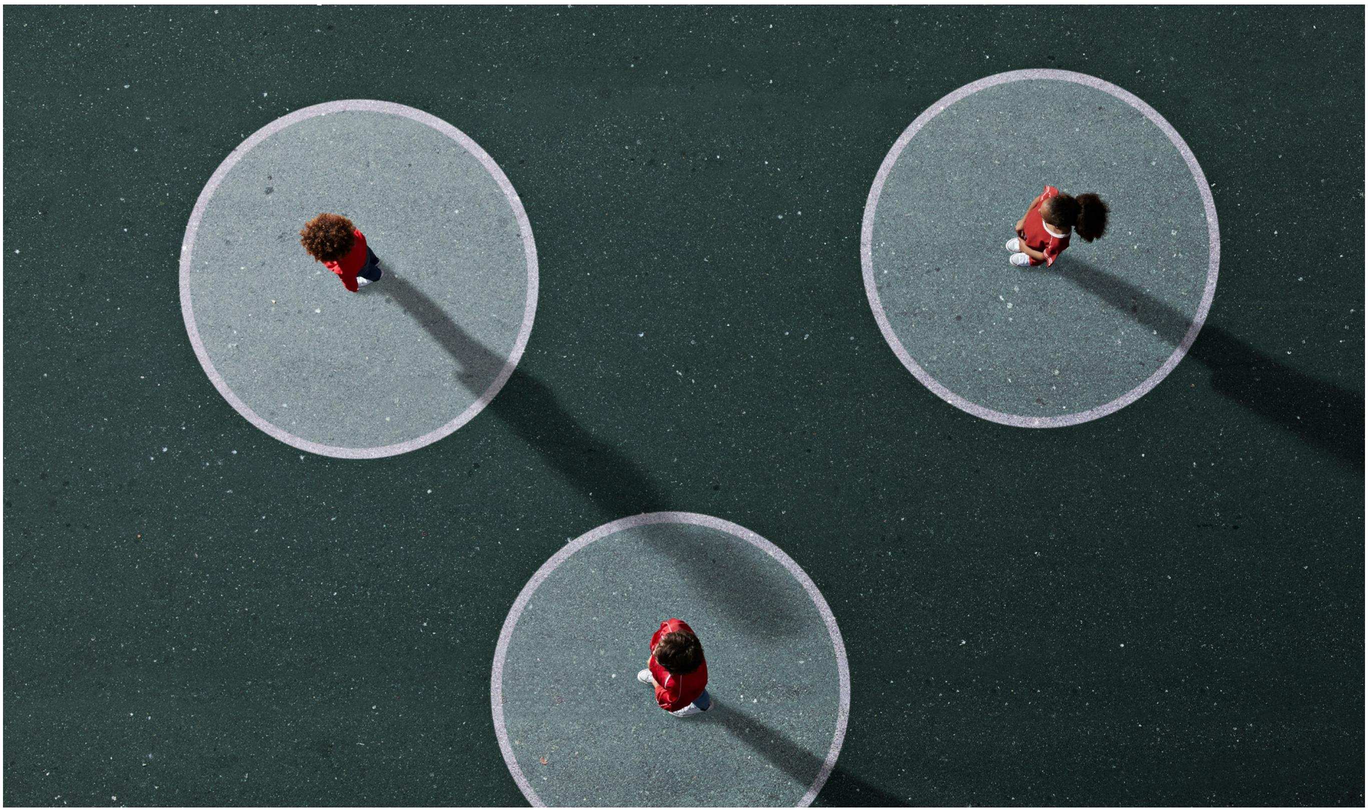
Where this extends to employees' family members, for example, where an employee tells their employer that a family member is classed as a vulnerable or extremely vulnerable individual, the employer will need to consider how it can inform them about its processing of their personal data in line with its transparency obligations under data protection laws.

✓ 6. Exercise of rights

Individuals, including employees have a suite of rights under data protection laws and data subject access requests are frequently submitted by employees to their employer to try to elicit information that will support potential claims. As a result, employers should bear in mind that any personal data retained during the COVID-19 pandemic may have to be provided to employees in response to future requests.

Businesses should ensure that staff are able to exercise their information rights in relation to the personal data collected during the COVID-19 pandemic. Ideally, employees should be able to exercise their rights in an easily accessible manner, such as through a portal.

Businesses should update their procedures to factor in requests relating to personal data collected during the pandemic and references to the processing of this data will also need to be included in any response letter to a subject access request.



Conclusion

The ICO has made it clear that, as a pragmatic regulator, it recognises the acute stresses businesses are currently facing due to the COVID-19 pandemic, and that it will not unduly penalise those who have difficulty in complying with their obligations under data protection laws due to a lack of financial or other resources.

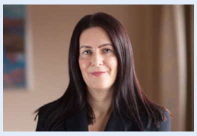
However, the ICO does expect businesses to do what they can to comply and crucially to take measures to ensure that their use of personal data is proportionate and fair. Factoring the key compliance measures described above into a return to work post-lockdown plan will go a long way towards ensuring that the correct balance is struck between the need to ensure the health and safety of the workforce and others and the right to privacy. This will also bring the added benefit of instilling confidence in employees that their personal information will be treated correctly, thereby ensuring that employees are fully aligned with the business's COVID-19 strategy.

Data Privacy Checklist

- ✓ Conduct and document Data Protection Impact Assessments.
- ✓ Embed data protection by design and default into the return to work plan.
- ✓ Comply with data minimisation.
- ✓ Update or supplement existing privacy notices.
- ✓ Review and update data protection policies and procedures.
- ✓ Update Records of Processing.
- ✓ Implement measures to ensure the accuracy and currency of data retained.
- ✓ Assess and document appropriate retention periods and audit their implementation.
- ✓ Review and implement appropriate technical and organisational data security measures, including setting appropriate access restrictions.
- ✓ If using service providers to process personal data, ensure that the necessary data protection terms are in place and audit their data protection compliance.

Our Data Privacy & Cybersecurity team are here to provide you with practical advice and support in dealing with the privacy issues raised by COVID-19 or any other privacy matters, both in the UK and across the globe. We are keen to assist you with your data privacy concerns.

Please contact the authors below or another member of our global Data Privacy & Cybersecurity team for a free initial consultation.



Francesca Fellowes
Director, Leeds
T +44 113 284 7459
E francesca.fellowes@squirepb.com

Emma Yaltaghian
Associate, London
T +44 207 655 1515
E emma.yaltaghian@squirepb.com

If you would like to keep up to date with privacy matters, subscribe to our Security & Privacy Bytes blog.

SQUIRE
PATTON BOGGS

squirepattonboggs.com