

# Workplace COVID Testing & Data Protection – Risk v Reward?

April 2020

# Workplace COVID Testing & Data Protection – Risk v Reward?

As the UK takes its first tentative steps out of the long, dark tunnel of the last year and the COVID-19 Pandemic, businesses across the UK are gearing up to welcome staff back to their desks, even if some may still continue to work from home at least some of the time.

The UK Government's been very clear in emphasising that workplace COVID-19 testing will be crucial to its plans for a gradual "reopening" of the UK economy, and businesses are being encouraged to play their own part in that process through employee lateral flow testing with the hope that this will help to reduce the spread of the virus and protect those who can't work from home.

"As many employers as possible" are being asked to commit to regular testing of their staff at least twice a week, even though participation remains voluntary. Those with less than 50 employees, sole traders and the self-employed have been encouraged to access community testing, and larger business given the option of setting up their own programmes or outsourcing to third-party providers.

Although some businesses may feel that a simple temperature check on entry may be the most straightforward way to manage this process rather than a more detailed regime involving the collation of lateral flow test results, collating any information which relates to the health and COVID status of an individual will involve the processing (though collection, further use and sharing it with third parties) of "special category" personal data, meaning that they'll also need to consider their data protection obligations.

It's worth noting that nothing in the UK GDPR (the new, essentially like-for-like version of the original EU GDPR adopted post-Brexit or the Data Protection Act 2018 prevents any business from taking any necessary and proportionate steps to keep their staff and stakeholder safe during the ongoing pandemic, but they will need to comply

with their terms to ensure that any data collected is dealt with lawfully, fairly, transparently and responsibly in line with the various data protection principles and enhanced requirements dealing with the collection and use of "special category" health data.

One of the key concepts of data protection regulation is "accountability" for how a business collects, uses and shares personal data – this is best demonstrated by having appropriate policies, procedures and processes in place to ensure compliance with its obligations. Amongst the raft of other risk assessments which Businesses will doubtlessly be carrying out, a Data Privacy Impact Assessment (DPIA – the Information Commissioner's template is available online) should be conducted before testing begins to focus specifically on data protection risk.

Given that "special category" health data is subject to additional protections, businesses should carefully consider whether or not lateral flow testing is genuinely necessary, based on their own specific circumstances. Many businesses will understandably want to "do their part" in the national effort to continue to flatten the Coronavirus Curve, but should ask themselves whether or not they truly need to collate COVID status information about their staff, whether this will actually help to provide a safe working environment and whether you could achieve your aims without the use of personal data.

Any specific health and safety, other regulatory requirements and duties of care may, for example, make COVID-testing essential for their operations as opposed to advisable or encouraged, and easier to justify.

Provided that you can show that you've adopted a reasonable, fair and proportionate approach and put in place the right arrangements to comply with your obligations, then data protection doesn't stop any business from

carrying out staff COVID testing, notably if your staff are on board with your proposals.

However, even if they are it's never a good idea to adopt a "one size fits all" approach to your testing programme; you may want to limit testing to high risk roles only and will need to ensure that access to any COVID status data is appropriately restricted on a genuine "need to know" basis.

Any collection and use of personal data will need to be based on one of the six lawful bases for processing referred to in data protection legislation; whilst testing is likely to fall under the specific lawful basis of "legitimate interest", which is by far the most flexible, that decision will need to be properly documented alongside your DPIA through a Legitimate Interests Assessment.

Additionally, as special category health data is considered inherently more sensitive, businesses will also need to identify a further condition for its processing, as set out in Article 9 of the GDPR – these include processing on public health and employment grounds.

If you do decide to roll out a staff testing programme, then it's extremely important to bear in mind your wider data protection obligations, including maintaining the security of any data collected and stored, being transparent with your staff through the introduction of a relevant workplace testing policy or privacy notice explaining to why their personal data is being collected, on what legal grounds, exactly how it will be used and how long it will be held for, ensuring that you only collect the absolute minimum of personal data necessary to achieve your objective. For example – the result of a relevant COVID test will be necessary, but information about other unrelated health conditions is far less likely to be.

Staff will also need to be able to raise any concerns over the operation of your testing programme and use of their personal data effectively and openly. Equally, if you choose to outsource your testing programme to an external provider, staff will need to be made aware of whom they are to ensure transparency and the

provider will need to enter into an agreement with specific obligations to regulate how they process and ensure the security of personal data on your behalf.

Once you're in possession of COVID test results and a list of which staff have either demonstrated symptoms or tested positive – whether staff provide you with their own test results or through the collation of your own – you can share that information with other staff, third parties and relevant Public Health or Local Authorities but should avoid naming any individual employee wherever possible and again only disclose the absolute minimum information necessary.

Public trust is central to the success of the UK's COVID-19 response, and rewarding the trust placed in a business by its employees when providing personal data through a workplace testing programme even more so. Much as we all may feel as if we're in this together, Blitz Spirit will not displace the importance of data protection in any business' response to the pandemic. Only through the responsible and compliant use of personal data will you be able to truly assess and manage your privacy risk, contribute safely to the UK's steady and safe pandemic exit strategy and avoid potential sanction by the Information Commissioner's Office (regardless of their stated temporary "flexible" approach) or the threat of civil claim by an aggrieved employee.

Testing times require exacting solutions, and we'd very much welcome the opportunity to help you develop and deliver them.

