APPENDIX

Key issues and practical steps for employers

An employer considering using tech tools to mitigate against Coronavirus in their workplace should be prepared to address the following key issues. This list focuses on the employer/employee relationship; similar issues concerning the use of tech involving customers, clients, contractors, supply chains and others are beyond the scope of this briefing.

- **What governance frameworks will apply?**
- **What do we want to achieve?**
- **How do we want to do it and what will that involve?**
- **Who will it affect and what might the impacts on them be?**
- **What are the risks to the business and its employees?**
- **How will we prevent or mitigate risks to the business and adverse impacts on our employees?**
- **How do we monitor and assess effectiveness?**
- **What is the end game?**
- **How do we engage with employees and deal with their concerns?**
- **How do we set up frameworks to react to developments (for example, government demands for information)?**
- **How do we communicate internally and externally?**

What governance frameworks will apply?

- Employers should not rush to implement a tech solution without first considering what they are trying to achieve and the benefits and risks which a particular solution presents in attaining that goal. Due diligence of the employer's full Coronavirus response strategy, and the place of tech solutions within that strategy, help assess the benefits to health & safety while identifying attendant risks to the business and its employees.
- Care should be taken not to silo the Coronavirus tech response to one area of the business. A Coronavirus task force or steering committee would promote a coherent approach across business functions and facilitate corporate leadership on a complex issue. It can also support unified messaging to employees affected by the company's response, allowing for transparency and, if designed appropriately, for the possibility of feedback from stakeholders on the approach taken to address Coronavirus.
- A clear governance framework should form the backbone of the deployment of any tech-based management of Coronavirus. Existing organisational risk management frameworks will provide the starting point, but the variety and novelty of the considerations raised by Coronavirus call for a cross-functional response that is appropriately tailored to identify and respond to the risks.
- The granular, issues-based risk assessments (discussed below) that will be components of the organisation-wide assessment should be co-ordinated and feed into the overarching framework.
- The design and conduct of these assessments should draw on the views and expertise of key internal stakeholders (e.g. DPO, HR, key board members, IT and cybersecurity teams) and may also require the support of external experts to design a framework for the deployment of tech-based measures that is effective, but minimises intrusion into, or impact on, the rights of employees. The skills of occupational health consultants, IT and data and/or human rights specialists should be considered.

- Initial assessments should be refreshed and revisited systematically to ensure that experiences gained and evolving facts inform revisions that may need to be made to the organisation's approach.

What do we want to achieve?

- There should be a clear set of objectives for the implementation of any tech-based solution aimed at tackling workplace issues thrown up by Coronavirus.
- Fundamentally, employers will want to create a safe workplace (covering both physical and mental health). Failure to take reasonable steps to do so can expose employers and senior management to litigation and enforcement risk. Employers will also want to ensure that any adoption of new tech solutions is pragmatically feasible, legally compliant and consistent with its organisational ethos and policies. The interests and concerns of employees will be a key consideration.
- It is particularly clear from the experience of government-imposed lockdowns that the workplace does not necessarily need to be the physical workplace. Testing and other tech carry the assumption that the present goal should be to get employees back into the office. But, for some employers, the best and most legally compliant course may be to keep employees working from home where it is possible to do so.
- What is necessary and appropriate is also likely to shift over time, depending on the intensity of spread of the virus, relevant government requirements and guidance and business imperatives. This means it is important to monitor and reassess measures taken and the shifting dynamics of the employer-employee relationship with evolving patterns of work and workplaces.

How do we want to do it and what will that involve?

- Once the organisation has identified its overarching objectives and the ways in which tech might facilitate achieving them, various assessments may be required to establish the practical steps forward and fine-tuning of plans, taking account also of regulatory frameworks within particular jurisdictions.
- In particular, these will include a health and safety risk assessment (HSRA) and, if the tech solution to be applied includes the gathering of data, a data protection impact assessment (DPIA). Although there will be overlaps with the steps taken to ensure compliance with applicable employment laws, employers should consider more broadly what the impacts of the use of tech might be on the rights of their workforce – while they may help secure rights to life, health and a safe workplace, there may be collateral adverse impacts on other rights, such as privacy. These can be identified and addressed through the incorporation of a human rights impact assessment, or HRIA, into diligence.
- For health and safety, existing regulatory frameworks will govern measures to be taken. These are being supplemented in a number of countries with Coronavirus-specific guidance. Having and appropriate risk-assessed safety measures in place, and communicating them, will not only be a vital component of legal compliance, but also critical in ensuring employee confidence in returning to the workplace.
- Contact tracing, surveillance and biometric testing all require the processing of employees' personal data. As a result, businesses need to ensure that they are compliant with GDPR (or equivalent local data legislation). A DPIA will examine, by reference to each tech solution contemplated, what data the organisation intends to process and why.
- As a first step, businesses should work out a data flow journey with outcomes for employees and third parties to assess how the technology works and what they want to obtain from it. For example, if the option of testing and tracking is considered:
  - at what point, and how often, will employees (or others on site) be subject to testing or tracking;

  - what personal data will be collected;
  - who will process it, i.e. will it be undertaken by the employing entity or outsourced to third parties (and how will diligence be undertaken on those third parties, including the security of the personal data);
  - who will see what data (e.g. will employers see all data revealed by a test or just positive/negative results);
  - who will be told about it (e.g. employees, the employer's Coronavirus task force);
  - what will be the consequences of difficult results (e.g. will employees or visitors be excluded from the building and for how long, and will this be used as a source of meeting obligations for notifying the relevant health and safety regulator of an instance of Coronavirus);
  - how will the use of data be audited, to ensure that the implementation of the measures mirrors the DPIA (and that any necessary modifications are addressed)?
- With biometric testing (e.g. temperature checks), health data (known as "special category" data) will be processed, meaning that it is important for businesses to collect and retain only the minimum amount of information (e.g. recording Coronavirus test results, but not details of pre-existing conditions). Particular rules are applicable to health data hosting services and the cautious approach that needs to be taken when subscribing to such services. For instance, in France, providers of health data hosting services must have a certificate of compliance and be approved by public authorities and a contract must be entered into with the hosting service provider.
- Under the GDPR, European businesses will need to consider whether they will rely on the employment condition or whether they can rely on a legitimate interest for the processing, show that the processing is necessary to achieve it, and balance it against the individual's interests, rights and freedoms. Many data regulators have made templates available to assist with that process. To the extent special categories of personal data such as biometric or health data are processed, more protective rules will apply, including with respect to the applicable legal basis (e.g. businesses will not be able to rely on their legitimate interest to process health data but will need to satisfy the special conditions set out in article 9 of the GDPR). In some jurisdictions, there are also requirements to consult employees or works councils in relation to measures taken.
- Less invasive technology (e.g. GPS or Bluetooth-triggered alerts when individuals are standing too close together) may be an additional part of the technology toolkit. Nevertheless, these technologies may be perceived as a restriction on freedoms of movement and subject to abuse, depending on application.
- The various assessments should tie into, and be consistent with, the overarching risk assessment framework to allow the organisation to make judgments on the optimal strategies to adopt, taking account of their particular circumstances, the risks to the business and the impacts on their employees.

Who will it affect and what might the impacts on them be?

- With almost any technological solution deployed to tackle Coronavirus, fundamental rights, such as privacy and freedom of movement, of all employees are at risk to a greater or lesser degree.
- An HRIA has a particular focus on the potential adverse impacts of the adoption and use of technology on employees. Whilst the aim of the technology will be to ensure worker health and safety, it is important to identify any potential adverse impacts on employees and the extent to which those may be avoided or mitigated. For example:
  - if the effectiveness of an app in identifying Coronavirus risk will be maximised by tracking on a 24/7 basis, what does this mean for employees' privacy outside working hours and for their right to a family life?
  - How is the Coronavirus response being tailored to take account of vulnerable workers?

- Adverse effects of a tool on employees who are more vulnerable (with respect to Coronavirus specifically, or otherwise) and who might be disproportionately affected by using the tech should not be overlooked.
- Protections (including in the form of tech) should be made available to employees on a non-discriminatory basis. If particular tools will be offered to some categories of employees and not others, consideration should be given to the justifications for this and how requests for expansion of access will be considered.
- Some tech may have design features or impacts that could operate in a discriminatory fashion. For example, in a temperature testing app, an elevated temperature may be due to IVF treatment or menopause, rather than Coronavirus, meaning that if employees wish to be admitted to the workplace, they would have to give additional information about their private lives (and being fixed with knowledge of this information may make employers vulnerable to discrimination claims). Options need to be built into the design of the technology (or the human handling of it) to avoid discriminatory outcomes.
- In order to keep the workplace safe, employers might also seek to apply tech solutions to visitors to premises, or contractors such as catering and cleaning providers. Conversely, contractors gaining access to the workplace may themselves seek to impose requirements or apply technologies that could impact on the work environment and personnel. Employers should take account of third-party uses of tech that might affect their staff.

What are the risks to the business and its employees?

- One of the headline risks will be that an employee (or a third party – such as an employee's family member) dies from Coronavirus and this is alleged to be as a result of the employer failing to put reasonable steps in place to provide a safe workplace.
- Another is that there is a data breach of personal health data, leading to enforcement action by data regulators and civil claims.
- There will also be a heightened cybersecurity risk (due to greater dependency on technologies, increased rate of cyber threats, network saturation) and a need to comply with cybersecurity regulatory requirements to ensure the security of the data.
- Increased technological surveillance may also give rise to long-term, unintended consequences, such as an irreversible shift in workplace culture, with increased interference in employees' private lives.

How will we prevent or mitigate risks to the business and adverse impacts on our employees?

- The various risk assessments should feed into an overarching framework that will allow the organisation to make judgements on the optimal strategies to adopt and the compliance and other steps required, taking account of their particular circumstances. The aim will be to take appropriate steps to prevent or mitigate any risks to the business and adverse impacts on employees.
- The HSRA frameworks will identify measures to overcome risks, and the role that technology will play in this. In this regard, governments and regulators have put in place guidance about measures to put in place, which is often sector-specific (for the UK, Government Guidance and HSE guidance is available).
- The DPIA should identify data risks, and any mitigating actions that can be put in place to counter the impact. Such actions might relate to the data set (e.g. deletion of data, anonymisation), the implementation of technological solutions, or engagement with employees. In addition:
  - A strict due diligence exercise will need to be conducted before entering into any contract with relevant tech providers to ensure compliant use of data and allocation of risks (e.g. to ensure that specific rules on health data hosting will be met).
  - Where businesses are working with third parties or other jurisdictions (e.g. providers of technology), data sharing agreements may need to be put in place to manage the safe sharing of data.

- To mitigate cybersecurity risks, employers can conduct training and raise awareness, test cyber resilience, adapt the group's cybersecurity compliance plans and procedures, adapt the group's cyber incident response plan, conduct strict due diligence exercises with third-party advisers/service providers, and consider cyber insurance coverage.
- Engagement with employee representative groups and employee surveys should alert employers if they are at risk of overstepping the mark with regard to the balance between safety, privacy and other considerations.
- Risk assessments should identify responsibilities and guidance for action in the event of unintended outcomes from the use of tech. For example, planning should address concerns around possible stigmatisation or discrimination against individuals affected by Coronavirus; heightened attention may need to be paid to reminding employees of other corporate policies; for example, in relation to social media and communications strategies and other measures to address possible data leaks.

How do we monitor and assess effectiveness?

- There may be several hallmarks of a successful Coronavirus management approach: a low Coronavirus infection rate amongst staff; a high level of take-up of tech; few employee complaints; a willingness to return to work; compliance with measures introduced.
- Tech itself can help monitor the effectiveness of wider workplace measures, depending on the features used. For example, GPS trackers on phones or wristbands can emit 'beeps' or signals when employees are standing too close together (and, depending on design, share that data with the employer), or lift surveillance can monitor whether people are abiding by distancing restrictions. Such measures should, of course, be scrutinised within the overarching risk assessment before being adopted as part of the overall response package.
- Metrics will depend on the workplace and workforce circumstances as well as the type of technology used – some will track behaviours and provide these to the employer, others will not. It is important that information on how well measures are succeeding is fed up to senior management (including board level, in some cases) as, ultimately, it is they who would be accountable for health and safety failings.
- In line with other risk frameworks within the organisation, an employer will want (and, in some cases, will be required) to keep a record of near misses, breaches and reportable incidents as well as concerns or complaints raised by employees (see below).
- It is important to create 'feedback loops' so that lessons learned from all monitoring and assessment processes inform adaptations and responses going forward.

What is the end game?

- It is a given that employers will want the workplace to have been safe, but how do they want to be perceived internally and externally as a result of their approach?
- Employers should consider and plan their policy approach to align with what they want their workplaces to look and feel like post-Coronavirus and the lasting impact of the technology to be.
- Do they want to retain the same traditional environment and associated culture, with enhanced surveillance (e.g. central buildings that are a permanent hub for employees, throughout the week)? If not, that may suggest that widespread investment in technology that is geared up to test, track and trace all employees at all times will not be appropriate.

How do we engage with employees and deal with their concerns?

- In some jurisdictions, employees or unions may be able to threaten to withdraw labour where they consider the workplace unsafe – and vulnerable groups may be particularly concerned about this. In others (for example, the UK), employees have a right to protection due to concerns over an unsafe workplace. Testing and tech can therefore seem an appropriate response to allay fears.

- Employers are likely to face legal challenge from employees if they seek to compel them to undergo testing, or if they threaten them with disciplinary action as a result, due to the sensitivity of the data involved, and the other potential options open to an employer (e.g. maintaining working from home, or question-based contact tracing). A consensual and reasonable approach is likely to be the most effective one.
- In many jurisdictions, engagement with works councils or employee representatives will be required – and, even if not required, can be a useful tool.
- Where businesses are working with third parties or other jurisdictions (e.g. providers of technology), data sharing agreements may need to be put in place to manage the safe sharing of data.
- Many employers will be proactive about encouraging individual employees to raise concerns, e.g. by issuing staff surveys. This will also help employers ascertain what the workplace should look like at different stages of the Coronavirus response and post pandemic. Consideration should also be given to dedicated communication lines for the submission of concerns or complaints and assurance that these will be addressed in a confidential and appropriate way. It will be important for employees to have access to channels through which to report any issues arising from the employer's tech response to the pandemic.
- Whistleblowers are likely to emerge in relation to concerns about the approach to tracking, testing and tracing – whether based on a belief that not enough is being done to keep the workplace safe, or that there are not enough safeguards in place around the use of data. Mechanisms which allow grievances to be aired will also give businesses an insight into where providing a remedy may be appropriate, if an individual has suffered from an infringement of its rights due to a business's approach.
- Some technology, such as workplace contact tracing, may be most effective if it also tracks colleague contact outside the office, e.g. in social settings. However, if that data is collected centrally by an employer, this would take data gathering much further into the private sphere. Employers must therefore balance their goal of achieving a safe workplace with the expectation of some retention of privacy. Tech solutions that offer a decentralised option (i.e. information is stored in the user's device, rather than a central employer databank) can be an appropriate option here.
- Regular awareness and training on relevant policies and practices developed in response to the Coronavirus pandemic should be provided to employees and others in the workplace.

How do we set up frameworks to react to developments (for example, government demands for information)?

- Organisations must keep their approach proportionate and fluid as the Coronavirus response unfolds and should be transparent about any changes in approach.
- Data regulators globally are addressing the emerging use of technology, so it is important to keep abreast of emerging guidance. It should not be assumed that what is acceptable in one jurisdiction can be imported to others.
- Within the taskforces or other governance structures established to deal with the Coronavirus response, responsibility should be allocated for keeping up to date with market trends, peer action and legal developments, so that organisations are poised to engage, when appropriate.

How do we communicate internally and externally?

- Consent and transparency are critical issues: businesses will need to communicate and engage with employees and third parties to explain their approach to the use of new tech (and consult with unions, works councils or other representative bodies, if necessary). They should be ready to explain how and why they wish to process the data, ideally in the form of privacy notices, and provide employees with an opportunity to raise any concerns and explain how those concerns will be handled.