ISSUES TO NOTE DURING COVID-19 CRISIS

Contracts

Organisations could find it difficult to fulfil its contractual obligations, and to avoid being held liable for a failure to comply with these obligations, companies should review the "force majeure" clauses within your commercial contracts to ascertain if COVID-19 is a designated "force majeure event". If so, what requirements will need to be satisfied to successfully invoke the force majeure clause to protect the interests of your organisation.

Insurance

Is your business insured against disruption?

Policies should be reviewed to ascertain the insurance coverage to mitigate losses related to the outbreak in the interim and longer term. Detailed consideration should be given as to what events are covered, either directly or indirectly, as well as any limitations, extensions and exclusions. It is crucial to check the extent of cover in each policy and, where unclear, to clarify it with your broker. Some key heads of cover to look for in your insurance portfolio are set out below:

- Business Interruption

  These policies typically cover income lost as a result of damage to or physical loss of property so the terms of such a policy should be reviewed carefully for their application to the current situation where interruption has been caused by the outbreak of infectious disease, COVID-19 since 28th February 2020.

- Employer's Liability

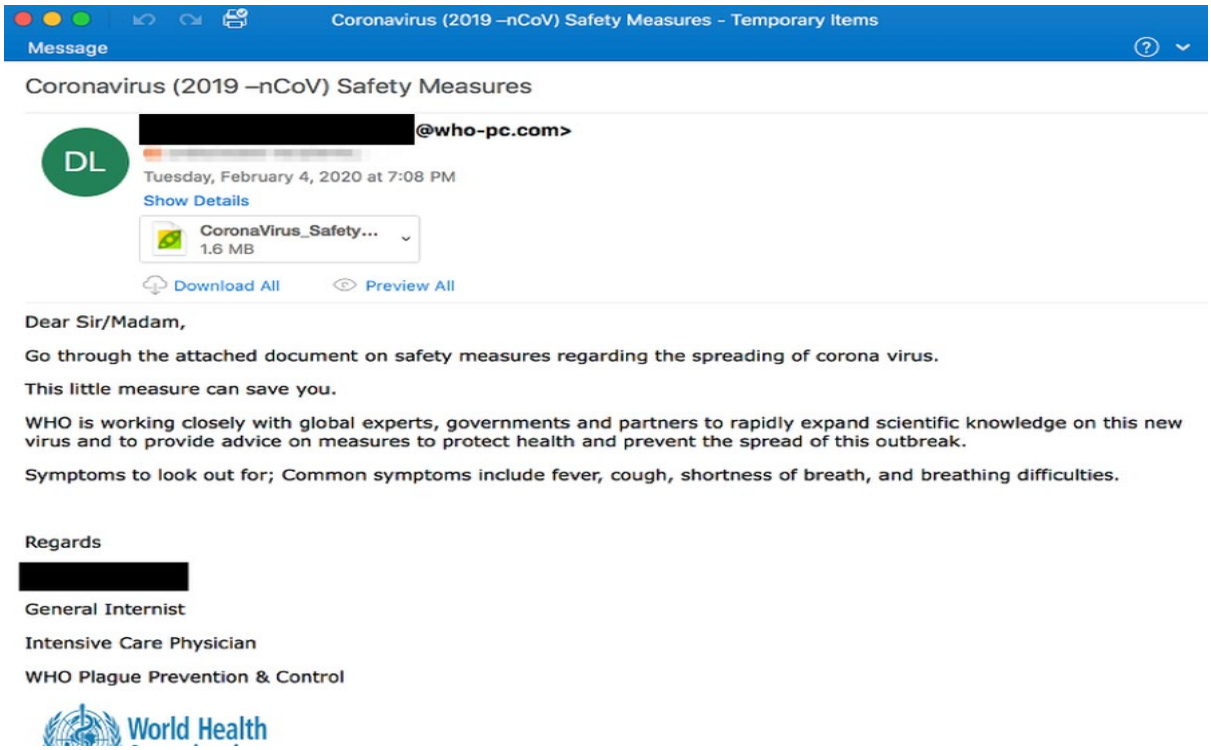
  Employer's liability insurance can provide cover for businesses which become liable for damages, costs or expenses to their employees as a result of injury sustained in the course of employment. Policy wording should be checked for extension of cover to disease and duties imposed on the insured such as preventative and precautionary measures and compliance with statutory requirements and health authority advice.

Where staff are working from home, employers continue to have obligations in relation to their health, safety and welfare. This means that employers can be liable for injuries sustained in the course of an employee's work even if sustained in a location beyond the ostensive control of the employer. Businesses that expect part or all of their workforces to work from home should carry out a risk assessment of the work activities involved and any possible risk reduction measures. Insurance cover should be checked for any exclusions or extensions in relation to working from home.

Cybersecurity

There has been an increase in hackers exploiting coronavirus fears as cyber-attacks sour. Phishing is a type of cyber-attack in which scammers send malicious messages that appear to be from a trusted source.

Last month IBM discovered a series of coronavirus-themed phishing scams attacks targeting Japanese organisations. At the time, the country was the second-worst affected by the disease, but as the infection has spread, so has the scope of the scam. The bogus emails exploit coronavirus-related fears in several ways. Many of them, such as the example below, prey on people's desire to find guidance on how to stay safe:



It would be advisable to run, or increase, penetration testing and training of staff with regards to these types of cyber-attacks.

Also, hackers are now aware that a lot of employees will be working at home and may not have the same level of security on their PC/laptop that your company policies insist upon. Therefore, making it easier to hack into your systems, so where possible IT security should be rolled out or if not possible, then other security measures would be required to be increased.

Data Protection Document Framework

Temporary policies should be created to cater for this crisis:

- A Working from Home Policy should be developed and implemented if one is not already in place that can establish appropriate boundaries between work and home activities during this period. The working day may need to be adjusted if employees have to tend to sick children, partners, or spouses etc. or if their children need to be cared for during the day.

- A Bring Your Own Device (BYOD) Policy may need to be developed and implemented if one is not already in place. If you require home workers to use their own equipment, i.e. laptop and phone, this is referred to as BYOD. The main problem with this is the lack of control and the increased risk of data breaches. The lack of control occurs because the company will have no control over patch management and ensuring security vulnerabilities are fixed. Breaches may occur because of the increase in hacking activity during this pandemic due to the lack of, or low-level IT security on these machines; or staff downloading apps or visiting sites that the company would normally blacklist in order to protect against infected malware, therefore putting the company information at risk.

- Review your IT security policy and note any amendments required for this COVID-19 period.

- Providing/amending privacy notices - The DPC have indicated that employers are likely to be justified in asking employees (and other visitors to their premises such as suppliers and contractors) to confirm whether they have been in a COVID-19 affected area or are experiencing COVID-19 symptoms. Where organisations intend to implement more intrusive measures (such as, for instance, employee and visitor questionnaires), these may still be justified; however, there should be a clear (and preferably documented) justification for doing so.

  The DPC indicated that the legal basis for processing in the context of the COVID-19 epidemic is likely to fall within the scope of Article 9(2)(i) of GDPR (and Section 53 of the Data Protection Act 2018), which provides for the processing of special category/health data by organisations where it is 'necessary for reasons of public interest in the area of public health'. The DPC points to this justification for processing as being appropriate in the context of acting on the guidance and directions of public health authorities.

  Employers may also have a legal basis to process personal data under Article 9(2)(b) of GDPR where such processing is carried out in accordance with their legal obligation to protect their employees under the Safety, Health and Welfare at Work Act 2005 (as amended). Furthermore, in emergency situations, there is a legal basis to process personal data, where necessary, in order to protect the vital interests of a data subject.

  In addition to the requirement for processing to be necessary and proportionate (as noted above) the DPC have made it clear that organisations will still need to ensure that they implement suitable safeguards and security measures to protect the data subjects concerned. At a minimum, these measures should include:

  (i) minimising the personnel who have access to the personal data;

  (ii) putting in place strict retention policies and time limits in respect of any personal data processed;

(iii) ensuring that staff are adequately trained in the protection of data subjects' personal data;

(iv) putting measures in place to ensure the confidentiality of employees' personal data, particularly where health data is concerned; and

(v) being fully transparent with employees in relation to the personal data which is processed and the reasons for such processing.

In order to maintain accountability and demonstrate compliance with GDPR, organisations should document their decision-making processes in relation to personal data processing measures taken to control and manage COVID-19.

- Updating the risk register – ensure that all new, possible temporary risks are included in the risk register.

Remote Working

The Government has advised that employees should work remotely, where possible, and businesses should take a sensible approach in this regard. In general, remote working should be introduced (if possible) in line with any policy in place in the employment, and in consultation with employees. Employers should ensure the supply of equipment to enable employees to carry out their duties remotely. The arrangements for the management and supervision of employees working remotely should be considered, along with issues such as the protection of confidential information, and any special insurance arrangements required. The health and safety and data protection implications of the arrangements should be considered. The Health and Safety Authority and the Data Protection Commission have both published guidance that will assist employers and employees in relation to working from home as part of the national response to COVID-19.

Remote Monitoring of Staff

Employees' monitoring even with a prior privacy notice might not suffice, under the GDPR. The scenario does not change with the remote monitoring of smart workers during the coronavirus emergency. Privacy rights of employees are protected and the principles are as follows:

- it is not possible to continuous monitoring of employees;
- some monitoring activities can be performed, if necessary, to the performance of the working activity. But this can happen only after the provision of a privacy information notice, as well as the performance of data protection impact assessment and of a balancing test since the data processing activity, is likely to be based on legitimate interest.

However, if there is a suspect of illegal conduct perpetrated by the employee or of an activity damaging the rights of the employer, it is possible to access data (e.g., emails, log files etc.) to collect evidence of the challenged conduct, provided that a prior privacy information notice was given. And this scenario might be relevant in the current situation since a company might suspect that an employee is not working, and such a suspect might lead to an investigation on his behaviour

and device. It is crucial to have prior data protection notice that allows checks in such circumstances, also with the relevant DPIA and balancing tests, as otherwise, employees might be in a stronger position to challenge potential checks.

Communication of information

An employer's legal duties include an obligation to provide relevant information and instruction to employees. Communications to employees in respect of COVID-19 should be given in a form, manner and, as appropriate, language that is reasonably likely to be understood by employees. Communications should address guidance from Government and public health bodies on Covid-19, as updated.

If you require any assistance with your data protection legislation compliance, you can contact DPS on:

Mobile **087 2207471**

Email **ruth@dpsolutions.ie**

