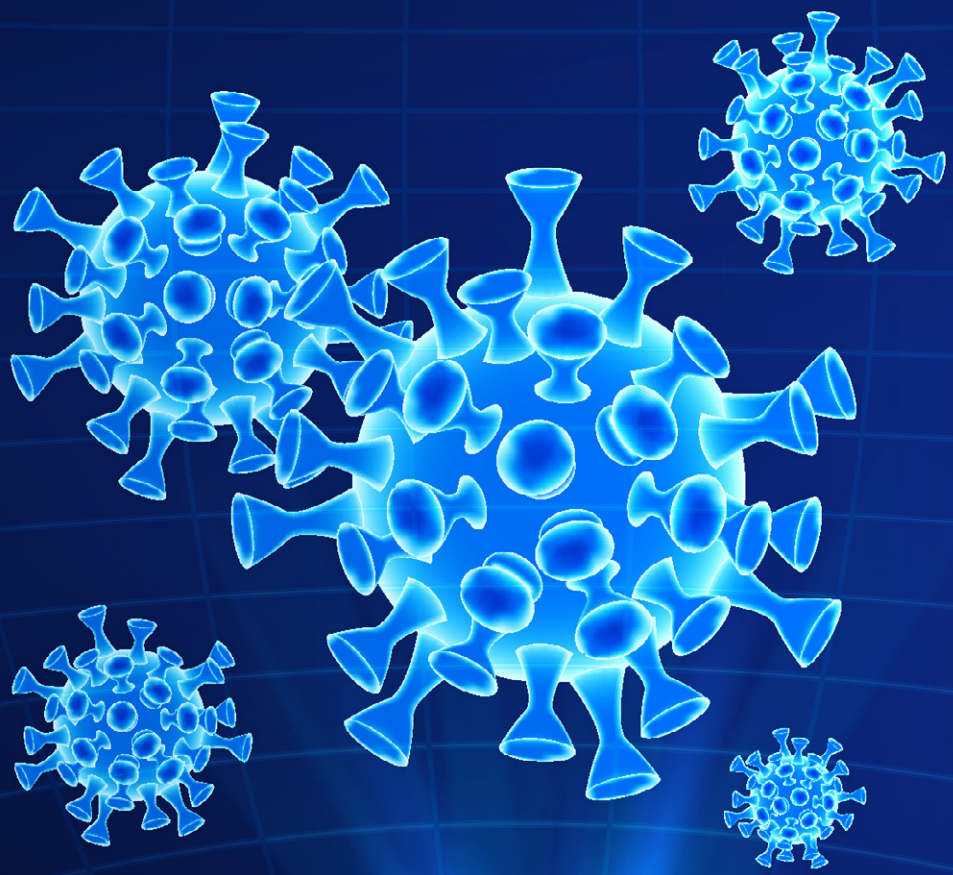
FLATTEN THE CURVE



CDH

CLIFFE DEKKER HOFMEYR

INDEX

Dispute Resolution

Can you cancel a contract because of COVID-19? 3

Avoiding contact, is there an easy way to sign documents electronically? 3

Working remotely: isn't there a risk? 3

Is business interruption (BI) insurance a COVID-19 lifeline? 3

For more information, please contact Tim Fletcher on tim.fletcher@cdhlegal.com

Corporate & Commercial

COVID-19: Compliance with the JSE Listings Requirements amidst the Pandemic. 4

- Should the impact of COVID-19 on businesses be announced, as price sensitive information? 4
- Are issuers required to publish trading statements, amidst the spread of COVID-19? 4
- Should the impact of COVID-19 on businesses be disclosed in their annual report, as a material risk? 4
- What to do should the spread of COVID-19 prevent issuers from publishing its financial results, in accordance with the JSE Listings Requirements? 5

How should issuers convene and conduct shareholders meetings, amidst the spread of COVID-19? 7

For more information, please contact Willem Jacobs on willem.jacobs@cdhlegal.com

Technology, Media & Telecommunications

COVID-19: Cyber security concerns 8

- Does your company have an information security or similar policy in place? 8
- Oh no, I was phished! What can I do? 8
- Can I be held liable for distributing 'fake news' about COVID-19? 9

What are some of the data protection implications of COVID-19 in South Africa? 10

For more information, please contact Christoff Pienaar on christoff.pienaar@cdhlegal.com

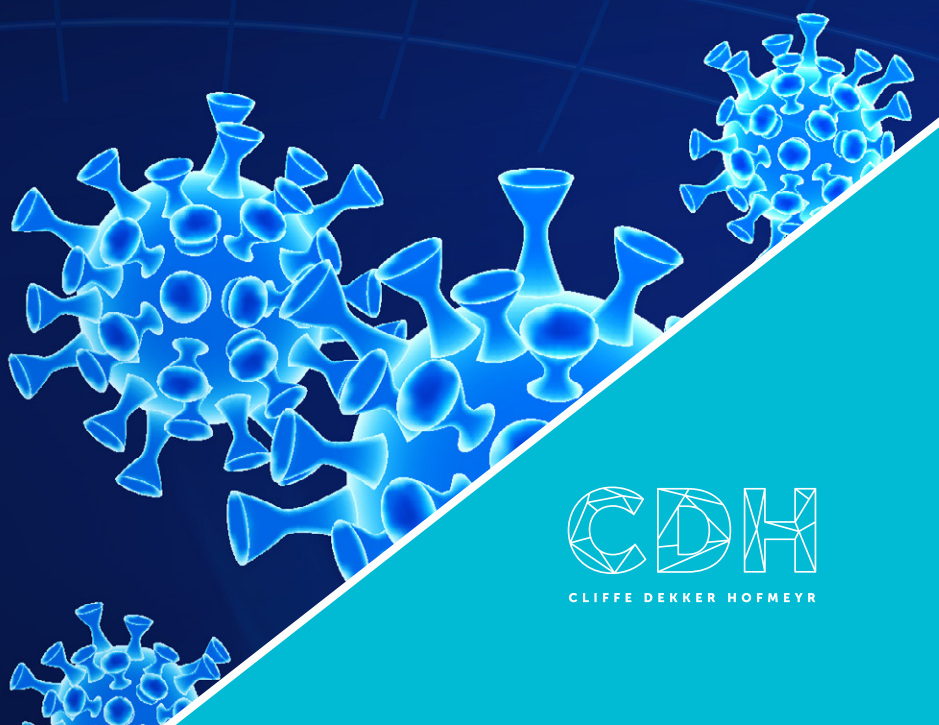
Dispute Resolution and Technology, Media & Telecommunications

Do flexible and remote working arrangements constitute a cybersecurity threat? 11

For more information, please contact Christoff Pienaar on christoff.pienaar@cdhlegal.com

DISCLAIMER:

The Survival Guide is an informative guide covering a number of topics, which is being published purely for information purposes and is not intended to provide our readers with legal advice. Our specialist legal guidance should always be sought in relation to any situation. This version of the survival guide reflects our experts' views as of 30 March 2020. It is important to note that this is a developing issue and that our team of specialists will endeavour to provide updated information as and when it becomes effective. Please contact one of the above directors should you require legal advice amidst the COVID-19 pandemic.



CDH

CLIFFE DEKKER HOFMEYR

Dispute Resolution

As we navigate the unchartered waters of COVID-19, we consider the potential points of impact on businesses

CLIFFE DEKKER HOFMEYR

Can you cancel a contract because of COVID-19?

Yes you can if it is objectively impossible to perform your contractual obligations and even in the absence of a *force majeure* clause in the contract. Importantly, each situation will depend on its own facts and the wording of the contract. Also, in the COVID-19 crisis specifically, developments must be considered carefully before concluding that there is an impossibility of performance or the triggering of a *force majeure* clause. Claiming impossibility or *force majeure* incorrectly could be a breach of contract and could give rise to a damages claim against you. In particular any impossibility of performance must be absolute and it is any event, including COVID-19 and its consequences, that could bring about an impossibility or *force majeure* provided it is unforeseeable with reasonable foresight, unavoidable with reasonable care and not the fault of either party.

A *force majeure* clause in a contract will take precedence over the common law and care must be taken to comply with any agreed time limits or process requirements set out in the contract.

Avoiding contact, is there an easy way to sign documents electronically?

Yes there is. Although there are important exceptions, electronic signatures are generally valid provided that the signature is specific to the person signing. That requirement can be satisfied by a message from that person's computer which includes a scan of their signature or simply adding a typed name, provided it is intended by the person to serve as a signature and acceptance of the content of the message. A contract signed in this way, again subject to specific exceptions, will be valid and enforceable.

There is a distinction between an electronic signature and an advanced electronic signature which is only available through an accredited agency and includes a secure process with specific software to secure the message.

Working remotely: isn't there a risk?

Certainly, the panic around COVID-19 will have cyber criminals licking their lips as more and more employees work from outside their usual office environment. Some IT environments are designed to cope with that kind of scenario, are very secure, with two-stage authentication including passwords that require change regularly, encryption and 24/7 monitoring. But that is not the norm. Where your service providers are handling your sensitive information, it is certainly prudent to check whether that information is secure both within that service provider's ordinary environment but particularly where people are accessing and processing your information remotely. With IT structures facing unexpected pressure, your enquiries should also include the backup arrangements employed by the service provider.

Where you are the service provider, it is self-evident that you must comply with your contractual obligations. Moreover when handling electronic information (especially personal information) and communicating electronically, you must act reasonably. Allowing external access to your systems without sufficient security by employees working from home is probably not what a reasonable business person would do and that could create an opportunity for cyber criminals. Where you act unreasonably and third parties suffer a loss as a result, you will be exposed to claims for damages.

Is business interruption (BI) insurance a COVID-19 lifeline?

BI insurance helps a business return to its financial position before a defined incident defined by the policy and may cover loss of revenue, wasted overheads and possibly even increased expenses where these are incurred to minimise loss.

Many BI policies cover an insured only for damage to property and proper analysis of the specific policy wording is vital to determine whether BI due to COVID-19 falls within the scope of the policy cover. Remember also the general duty to mitigate loss. Protocols to protect employees and ensure maximum business continuation may prove valuable when submitting a claim under a BI policy.

Coronavirus COVID-19 Global Cases by the Center for Systems Science and Engineering (CSSE) at Johns Hopkins University

https://gisanddata.maps.arcgis.com/apps/opsdashboard/index.html#/bda7594740fd40299423467b48e9ecf6

As we navigate the unchartered waters of COVID-19, we consider the potential points of impact on businesses

CDH
CLIFFE DEKKER HOFMEYR

COVID-19: Compliance with the JSE Listings Requirements amidst the Pandemic

The Johannesburg Stock Exchange (JSE) has issued a statement addressed to companies listed on the JSE, their sponsors and designated advisors to remind issuers of their continuing disclosure obligations amidst the disruption in the global economy emanating from the spread of COVID-19 (or the Coronavirus). Issuers, assisted by their sponsors and other advisors, are advised to properly investigate the actual and potential impact of the Coronavirus on their business and/or industry on an ongoing basis, to ensure that they are in a position to comply with their disclosure obligations under the JSE Listings Requirements, particularly the following disclosure obligations:

Should the impact of COVID-19 on businesses be announced, as price sensitive information?

An issuer must, without delay, unless the information is kept confidential for a limited period of time, release an announcement providing details relating, directly or indirectly, to such issuer that constitutes price sensitive information. Price sensitive information is defined in the JSE Listings Requirements as: "*unpublished information that is specific or precise, which if it were made public, would have a material effect on the price of the issuer's securities*".

In the JSE's Practice Note 2/2015, guidance is provided on what may constitute "*specific or precise*" information, and on how a "*material effect*" should be assessed. It further provides that directors of issuers are required to apply their own discretion in determining what will constitute price sensitive information, and if there is any uncertainty as to what constitutes price sensitive information, then the issuer's sponsor must be consulted. If doubt remains, the issuer must assume that the information is price sensitive in order to avoid selective disclosure which could lead to confusion in the market.

Are issuers required to publish trading statements, amidst the spread of COVID-19?

Issuers must publish a trading statement as soon as they are satisfied that a reasonable degree of certainty exists that the financial results for the period to be reported upon next will differ by at least 20% (or 15% for certain property entities which meet the criteria in paragraph 3.4(b)(vii) of the JSE Listings Requirements) from the most recent of the financial results for the previous corresponding period or a profit forecast previously provided to the market in relation to such period.

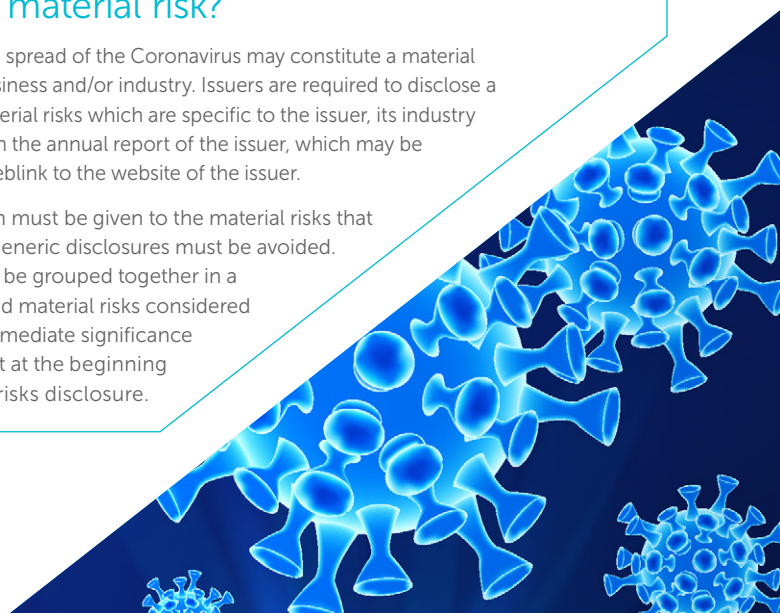
Issuers may publish a trading statement if the differences are less than 20% (or 15% for certain property entities which meet the criteria in paragraph 3.4(b)(vii) of the JSE Listings Requirements), but which are viewed by the issuer as being important enough to be made the subject of a trading statement.

Issuers are to ensure that they comply with the detailed requirements of paragraph 3.4(b)(i) to (viii) of the JSE Listings Requirements. Issuers who have a policy of publishing quarterly results will be exempt from these requirements, but must instead include a general commentary in each quarterly results announcement to ensure that shareholders are guided on the expected performance of the issuer for the next quarter.

Should the impact of COVID-19 on businesses be disclosed in their annual report, as a material risk?

For some issuers, the spread of the Coronavirus may constitute a material risk to the issuers business and/or industry. Issuers are required to disclose a description of all material risks which are specific to the issuer, its industry and/or its securities in the annual report of the issuer, which may be incorporated via a weblink to the website of the issuer.

Proper consideration must be given to the material risks that face the issuer and generic disclosures must be avoided. Material risks should be grouped together in a coherent manner and material risks considered to be of the most immediate significance should be prominent at the beginning within the material risks disclosure.



As we navigate the unchartered waters of COVID-19, we consider the potential points of impact on businesses

CDH
CLIFFE DEKKER HOFMEYR

COVID-19: Compliance with the JSE Listings Requirements amidst the Pandemic

What to do should the spread of COVID-19 prevent issuers from publishing its financial results, in accordance with the JSE Listings Requirements?

Issuers must, within four months after its financial year end, and at least fifteen business days before the date of its annual general meeting, distribute to shareholders and submit to the JSE a notice of the annual general meeting and the issuer's audited annual financial statements.

If an issuer has not distributed annual financial statements to all shareholders within three months of its financial year end, it must publish provisional annual financial statements within the three months as specified, even if the financial information is unaudited at that time.

In the JSE's statement, the JSE pointed out that due to the relevant national restrictions imposed on the country in which the issuer is domiciled, there may be an impact on an issuer's ability to comply with the JSE Listings Requirements, regarding inter alia the timeous publication and completeness of its financial results. The JSE does have discretion in this regard and have provided the guideline set out below to issuers who believe that they may not be able to comply with their financial reporting obligations.

Request for a Reporting Variation

The JSE have advised that considering the measures implemented in South Africa and globally to deal with the spread of the Coronavirus, where issuers believe they may not be able to meet their financial reporting obligations, issuers may request a variation of its financial reporting requirements (Reporting Variation) and the JSE shall consider such request on a case by case basis, in respect of:

(i) the timing of publication of interim, preliminary, provisional, annual financial statements and notices of annual general meetings, pursuant to paragraphs 3.15, 3.16(a) and 3.19 to 3.22 of the JSE Listings Requirements, respectively;

(ii) the completeness of interim, preliminary, provisional, and annual financial information pursuant to paragraphs 8.57 to 8.61 of the JSE Listings Requirements;

(iii) the completeness of the annual financial statements pursuant to paragraphs 8.62 and 8.63 of the JSE Listings Requirements; and

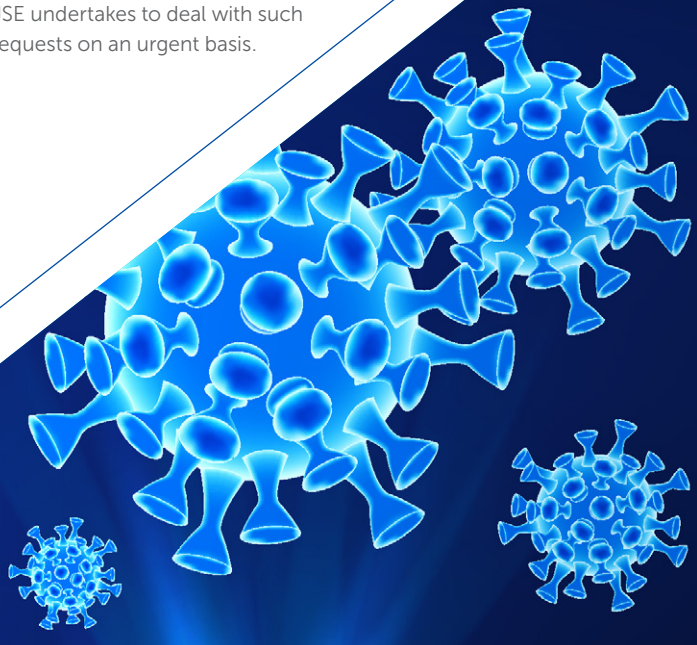
(iv) assurance reports by the independent auditor on the abovementioned information pursuant to paragraph 3.18 and 8.62(c) of the JSE Listings Requirements.

In the case of issuers that report to shareholders on a quarterly basis, where an issuer is no longer able to continue reporting on a quarterly basis, issuers must give due consideration to the obligations of paragraph 3.4(b)(i) to (viii) of the JSE Listings Requirements as the exemption from these provisions will no longer apply, to such issuer.

Notably, the JSE have warned that in requesting a Reporting Variation, issuers are urged to be responsible in their request so as to safeguard the principle of ensuring that sufficient, timely and reliable financial information is disseminated into the market to enable investors to make informed decisions. Where issuers are capable of providing certain financial information which will provide insights to investors in respect of financial position and performance such information should be provided in accordance with the JSE Listings Requirements.

The process of submitting a Reporting Variation request

The JSE advised that issuers are required to submit the following information under the event type "Ruling - Continuing Obligations" (for which no fee is payable) via its sponsor on the web based submission system WEBSTIR. Notwithstanding the period referred to in paragraph 16.3 of the JSE Listings Requirements, the JSE undertakes to deal with such requests on an urgent basis.



As we navigate the unchartered waters of COVID-19, we consider the potential points of impact on businesses

CDH
CLIFFE DEKKER HOFMEYR

COVID-19: Compliance with the JSE Listings Requirements amidst the Pandemic

What to do should the spread of COVID-19 prevent issuers from publishing its financial results, in accordance with the JSE Listings Requirements?*...continued*

The Reporting Variation request is to include the following information:

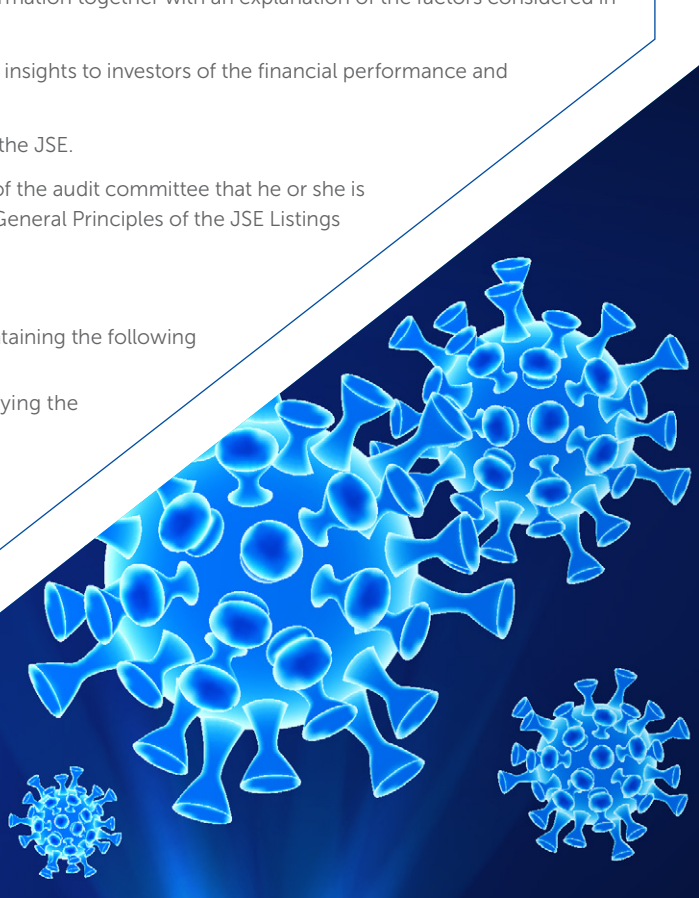
1. the appropriate matter set out under points (i) to (iv) above;
2. the reasons why the issuer cannot comply with the JSE Listings Requirements, to be detailed under one or more of the following headings:
    a. the ability of the issuer to generate financial information;
    b. the need for the issuer to reconsider the IFRS impact of the pandemic;
    c. the need for the issuer to seek external advice on (b);
    d. the ability of the issuer to provide sufficient appropriate evidence or information to the auditor;
    e. the ability of the auditor to complete or perform their assurance engagement; and
    f. any other practical impediment relevant to the financial reporting requirements of the issuer;
3. for each of the items identified in (2) above:
    a. the manner in which the issuer intends to address each of these items; and
    b. the expected timing of publication of the relevant financial information together with an explanation of the factors considered in determining the estimated date of reporting;
4. details of the financial information that can be published to provide insights to investors of the financial performance and position as discussed in 2 above; and
5. any other information the issuer wishes to bring to the attention of the JSE.

The request must be accompanied by a statement signed by the chair of the audit committee that he or she is in agreement that the request will assist the issuer in ensuring that the General Principles of the JSE Listings Requirements are upheld.

Disclosure of the Reporting Variation

Should the JSE agree to an issuer's request, a SENS announcement containing the following minimum information is required to be published by the issuer:

- the nature of the Reporting Variation that has been agreed, identifying the matter and the variation granted;
- a summary of the reasons provided to the JSE underpinning the request for the Reporting Variation; and
- the expected timing of the normalisation for the issuer's reporting obligations as agreed with the JSE.



As we navigate the unchartered waters of COVID-19, we consider the potential points of impact on businesses

CDH
CLIFFE DEKKER HOFMEYR

How should issuers convene and conduct shareholders meetings, amidst the spread of COVID-19?

The JSE has issued a further statement addressed to issuers convening and conducting its shareholders meetings, amidst the spread of the Coronavirus.

The JSE reminds issuers, domiciled in South Africa, in accordance with section 63(2) of the Companies Act 71 of 2008 (Companies Act), that unless prohibited by the issuer's memorandum of incorporation:

- a shareholders meeting may be conducted entirely by electronic communication; or
- one or more shareholder, or proxies for shareholders, may participate by electronic communication in all or part of a shareholders meeting that is being held in person.

In order for an issuer to conduct a shareholders meeting, in accordance with section 63(2) of the Companies Act, the electronic communication employed must ordinarily enable all persons participating in that meeting to communicate concurrently with each other without an intermediary and the electronic communication must also enable all persons to participate in the meeting in an effective manner.

Every shareholders meeting of a public company must be reasonably accessible for electronic participation by shareholders, in accordance with section 61(10) of the Companies Act. Considering the spread of the Coronavirus, should the issuer wish to hold their shareholders meeting entirely electronically, the only requirement is that the notice of shareholders meeting provides the following: (i) the availability of electronic participation; (ii) the necessary information to enable access to the medium of electronic communication; and (iii) that the access to the medium of electronic communication is at the expense of the shareholder or proxy, except to the extent the issuer determines otherwise.

If notice of a shareholders meeting has already been dispatched, without providing for the meeting to be held entirely electronically as above, the issuer will need to provide all shareholders notice of such detail, reasonably in advance of the meeting, using the prescribed modes of delivery and the deemed delivery provisions set out in Table CR3 of the Companies Regulations, 2011. For example, such notice may be posted to shareholders and will thereby require the issuer to provide for 7 calendar days for deemed delivery. Unfortunately, a SENS announcement will not suffice. What constitutes "reasonably in advance" is unclear but could for example, after consideration by the board of directors of the company, be set at 72 hours in advance of the shareholders meeting.

Given the nation-wide lockdown for 21 days with effect from midnight Thursday, 26 March 2020, it might however not be possible or practical to arrange for notices to be delivered in the prescribed manner during this period.

The Companies Act does not provide for a mechanism in which the company is able to postpone the shareholders meeting in advance of the meeting, other than at the meeting. Usually, should a quorum not be met at the shareholders meeting, the meeting is adjourned in accordance with section 64 of the Companies Act. Should an issuer be unable to co-ordinate a fully electronic meeting within the lockdown period, in accordance with the above, issuers do have the option of unilaterally cancelling the shareholders meeting altogether and to reconvene a shareholders meeting by issuing a new notice of shareholders meeting to shareholders.

The JSE has not elaborated on the conduct of shareholders meetings considering the impact of the Coronavirus for issuers not domiciled in South Africa. We therefore recommend that should the applicable laws of such issuers place of incorporation provide for shareholders meetings by electronic participation, such method should be considered.

We remind issuers to engage with their sponsors and/or designated advisors should there be further uncertainty around conducting and convening its shareholders meeting, amidst the spread of the Coronavirus.

As we navigate the unchartered waters of COVID-19, we consider the potential points of impact on businesses

CDH
CLIFFE DEKKER HOFMEYR

COVID-19: Cyber security concerns

As a response to the outbreak and increasing number of COVID-19 cases, more companies and organisations are encouraging or instructing employees to work remotely. With an increased reliance on technology due to remote working arrangements, entities may be faced with cybersecurity challenges including cyber-attacks and cyber-related fraud. We outline some considerations for organisations below.

Does your company have an information security or similar policy in place?

We advise all organisations to review their information security policies and to educate employees on best practice. Of particular relevance in the present circumstances should be organisations' incident response plans and how the organisation will react in the case of a data breach or cyber-attack. Policies should outline practical steps which employees can take in the event of an alleged or actual data breach or cyber attack, including who to contact and the contact details of that person(s), the procedure for escalation and how to minimise losses.

We recommend that organisations circulate their incident response plans and information security policies to employees and draw attention to the relevant provisions to ensure employees are familiar with the steps to follow. To the extent that an organisation does not have a policy or response plan in place, we recommend drafting basic guidelines which are specific to the current challenges posed by COVID-19 and which addresses the most pressing and important risks which may arise, and circulating this as soon as possible.

Organisations should actively monitor the relevant regulatory authorities for updates or changes regarding COVID-19 and ensure that their policies and plans are updated to align with the latest official rules or recommendations from credible institutions such as the Centre for Disease Control and Prevention, the relevant government authority or the World Health Organisation. This may include updates to the number of days an employee should self-quarantine if they have potentially been exposed to COVID-19, the number of persons that may congregate at the office at the same time, or the manner in which COVID-19 is transmitted.

Oh no, I was phished! What can I do?

You should immediately report any fraudulent activity to your IT department and change all of your passwords and restart your computer.

If you are worried that you or your business are at risk as a result of the phishing incident or someone has hacked into your system or is holding some of your data ransom, you should report this to the South African Police Services and ask them to open up an investigation. You should work with your company and consider hiring an IT security company or private investigator that specialises in cybercrime investigations to assist you.

Phishing, hacking, identity fraud and computer-related extortion are currently offences under sections 86 and 87 of the Electronic Communications and Transactions Act 25 of 2002. A person found guilty of these offences faces a fine or imprisonment of up to 5 years. A fraudster can also be tried for fraud and theft under the common law.

If you are able to locate the perpetrator, you can also bring a delictual claim against them and receive monetary compensation for any financial losses suffered. You can also bring an interdict against the perpetrator to prevent them from sharing any of your data and get them to return data that is in their possession to you.

As we navigate the unchartered waters of COVID-19, we consider the potential points of impact on businesses

CDH
CLIFFE DEKKER HOFMEYR

COVID-19: Cyber security concerns

Can I be held liable for distributing 'fake news' about COVID-19?

The publication and dissemination of 'fake news' in South Africa is not generally prohibited but new regulations published under the Disaster Management Act, 2002 on 18 March 2020 regarding COVID-19 state that *"any person who publishes any statement, through any medium, including social media, with the intention to deceive any other person about (a) COVID-19; (b) COVID-19 infection status of any person; or (c) any measure taken by the Government to address COVID-19, commits an offence and is liable on conviction to a fine or imprisonment for a period not exceeding six months, or both such fine and imprisonment."*

The intention of the regulation is to avoid the malicious spreading of false news and unnecessarily creating panic in the public. The public should critically review information it receives about COVID-19 and the source of such information. The above quoted regulation is limited to the publishing of any statement regarding COVID-19 and not generally to 'fake news' (in the colloquial understood sense).

When sharing information regarding COVID-19 on social media, it is imperative to ensure that this information is obtained from accredited institutions such as official government channels of communication, medical journals, the World Health Organisation or the Center for Disease Control and Prevention.

To quote the director-general of the World Health Organisation, Tedros Adhanom Ghebreyesus, "*We're not just fighting an epidemic; we're fighting an infodemic. Fake news spreads faster and more easily than this virus, and it [is] just as dangerous*".

As we navigate the unchartered waters of COVID-19, we consider the potential points of impact on businesses

CDH
CLIFFE DEKKER HOFMEYR

What are some of the data protection implications of COVID-19 in South Africa?

In order to mitigate the spread of COVID-19 in South Africa, both public and private organisations will be required to implement data-sharing strategies and procedures in respect of COVID-19-related personal information. Organisations in the European Union – the current epicentre of the COVID-19 pandemic – are already in a position to implement such data-sharing strategies after having received guidance from European data protection regulators.

Notably, both the Information Commissioner's Office (ICO) in the United Kingdom and the Data Protection Commission (DPC) in Ireland have issued statements in order to clarify the position on data protection in the context of the COVID-19 pandemic. These statements stress that European data protection laws are not crafted to prohibit the sharing of personal information in order to protect against serious threats to public health – such as COVID-19. Accordingly, organisations to which European data protection laws apply should not restrict themselves from taking the necessary action in response to the COVID-19 pandemic, provided that they continue to comply with data protection principles – particularly those in relation to ensuring that the personal information being processed is secure (i.e. by taking reasonable technical and organisational measures to prevent such personal information from being unlawfully accessed, lost or damaged).

Similarly, South African organisations are going to be required to balance common law and constitutional rights to privacy in the current circumstances by taking into account the provisions of the South African Protection of Personal Information Act, 2013 (POPI), which is relevant, although not yet fully in force, in regard to how they will lawfully process COVID-19-related personal information. POPIA provides for the legal basis on which personal information may be processed. The best solution is to obtain the person's consent and, given the sensitive nature of this information, to take the necessary steps to ensure that the personal information is safeguarded and kept secure, is not used for any other unrelated purpose and that it is not retained for longer than such information is required. Where it is not possible or practical to obtain consent, POPIA provides for instances of specific authorisation for the processing of health data which include that it allows for *"processing by...medical professionals, healthcare institutions or facilities or social services, if such processing is necessary for the proper treatment and care of the data subject, or for the administration of the institution or professional practice concerned"*.

Other organisations who are required to process COVID-19-related personal information could also potentially rely on the general authorisation that the processing of such health-related personal information is *"necessary for the establishment, exercise or defence of a right or obligation in law"* – provided that the organisation in question can show that the processing in question took place in accordance with a specific law.

While it will generally be lawful for relevant South African organisations to carry out reasonable processing of COVID-19-related personal information in the current circumstances, considering the increased cyber security risks that are presenting themselves during the COVID-19 pandemic, organisations processing COVID-19-related personal information (e.g. of their employees) should take necessary steps to ensure that the relevant COVID-19-related personal information is kept secure and that the privacy rights of individuals impacted by the virus are protected.

As we navigate the unchartered waters of COVID-19, we consider the potential points of impact on businesses

CDH
CLIFFE DEKKER HOFMEYR

Do flexible and remote working arrangements constitute a cybersecurity threat?

The era of the millennial workforce and the rise in technology and connectivity has required a dynamic shift toward flexible and/or remote working arrangements in South African corporate spaces. These flexible working arrangements, which are designed to depart from the notion that employees need to physically attend the office during traditional working hours, usually envisage scenarios where employees can clock in their hours from the comfort of their own homes, a coffee shop or even abroad. As a response to the COVID-19 pandemic, more companies and organisations are encouraging or instructing their employees to work remotely.

With an increased reliance on technology due to remote working arrangements, companies may be faced with cybersecurity challenges including cyber-attacks and cyber-related fraud. Despite cyber security software that may be available to employees, there is an added inherent risk in accessing a company's network from any location other than the workplace. Employees who work remotely and use public networks whilst doing so, such as the free WIFI available in cafés or airport lounges, are therefore vulnerable to the increasing threat of cyber-attacks.

The most common forms of cyber-attacks include the interception of email correspondence and phishing scams. This often occurs when cybercriminals monitor the servers of either the sender or recipient of an email communication and strategically intercepts the communication by posing as a sender.

Employees should also be aware that there has been an increased number of reported phishing scams on email related to the COVID-19. There are reports of fraudsters impersonating agencies such as the World Health Organization, a company's human resources department or other government agencies enticing people to open up attachments or to click on links with information regarding COVID-19. Attackers are then able to push malware, ransomware and attempt to gain access to a personal information and passwords.

Email interception, hacking, identity fraud and computer related extortion are recognised as offences under the Electronic Communications and Transactions Act No 25 of 2002 (ECT Act), and the maximum penalty is a fine (unspecified) or imprisonment for a period not exceeding 12 months. The Cybercrimes Bill [B6 of 2017] will, once effective, create a variety of new offences which do not currently exist in South African law and afford companies with a degree of comfort relating to the prosecution of cybercrime offences.

Although South African law currently does not specifically impose a duty to implement cybersecurity measures in an organisation, the Protection of Personal Information Act No 4 of 2013 (POPI Act) (the substantive provisions of which have not yet commenced) does contain obligations on responsible parties (data controllers) to implement reasonable technical and organisational measures to safeguard personal information in their possession or control against unauthorised access, which will likely include adopting cybersecurity measures.

According to the latest annual Cost of a Data Breach Report, conducted by the Ponemon Institute, the average cost of a data breach in South Africa is approximately R43,3 million. As a result, flexible and remote working arrangements may pose a substantial and costly risk to employers from a cyber security perspective.

Against this backdrop, it is imperative for business to review and adopt an information security policy which employees must adhere to. Employees should be encouraged not to connect to unsecure or public WIFI and utilise, where applicable, VPNs to protect their company's proprietary information. Common sense should also prevail, employees should check URL's before clicking on any links and beware of suspicious emails. With an increased use of teleservices such as Skype, Microsoft Teams, Zoom and the like, employees should ensure that meeting requests are legitimate prior to joining any meeting and refrain from taking 'shortcuts', such as sending documents to colleagues via unsecured instant messaging services, discussing confidential work matters on public chat platforms, saving documents to their desktop instead of on secure locations and using unencrypted personal devices for work matters. Any work should occur via the employer's designated channels for remote working, such as VPN's or servers.

Companies should insist that any remote working arrangement should occur via its designated digital channels for remote working, such as VPN's or servers.