Lawyers | McCullough Robertson

COVID-19

A McCullough Robertson resource guide

FAQs

Q: How can I close down my operations until the COVID-19 crisis is over, so I can quickly reopen afterwards?

A: We recommend the following steps –

I. State Governments are starting to introduce new temporary laws which will enable them to prevent landlords from terminating leases or retaking possession of leased premises for the next six months. You should **check whether such laws apply to your lease**. Then talk to your landlord. Explain to them that you are temporarily closing your operations, but intend to reopen when possible. Ask them to agree to not charge you rent for a period of time – i.e. for up to six months. Many landlords will agree to a full or partial rent reduction. Depending on the terms of the lease, if you are prevented by the new laws from operating from the leased premises, the lease may be 'frustrated' and discharged at law. Whether a lease can be 'frustrated' as a result of consequences arising from COVID-19 is yet to be tested. You should seek legal advice if you want to try to get out of the lease altogether.

II. Talk to your **bank or other lenders**. Most banks have already announced they will defer loan repayments for small businesses affected by COVID-19 for six months. For further details on how to apply see here.

III. Work out how you will **deal with employees**. There are options available other than making them redundant – see 'What about employees?' below.

IV. Talk to the **Tax Office** about obtaining an extension of up to six months for the payment of any tax liabilities. Your tax agent can seek this extension on your behalf. Ensure that you continue to lodge any activity statements or other returns on time if possible.

V. Talk to your **utility providers** about an extension of time to make any payments due. Most utility providers are willing to grant extensions for payment.

VI. Talk to your other **creditors (i.e. suppliers)**. Changes to the law commenced on 25 March 2020 which will make it difficult for unsecured creditors to seek to recover their debts for the next six months – see here. However, we still recommend you discuss with all your creditors how you will seek to repay them once the COVID-19 crisis is resolved. Creditors need to understand that it may take some time for revenues to come back and that payments may be delayed even after trading resumes and so extended payment terms will be necessary.

VII. Investigate and apply for any **Commonwealth Government assistance** that is available. Details of the current assistance available can be found at –

- https://treasury.gov.au/coronavirus/businesses
- https://treasury.gov.au/coronavirus/business-investment
- https://treasury.gov.au/coronavirus/sme-guarantee-scheme
- State and Local Governments are also providing assistance.

VIII. Start working on a plan now as to how you will **secure new supply on credit and pay new debts incurred and existing creditors** when you recommence operations and the restrictions on creditors pursuing their debts is lifted. Honest and open communication with all creditors about this is important so that everyone understands each other's position and expectations.

IX. Keep your **accounts and financial records up to date** so they are accurate and you know exactly what you owe and what you are owed.

FAQs

Q: If I continue to trade and incur debts that the company can't pay, will I be breaching the insolvent trading laws?

A: No. The **insolvent trading laws will not apply for six months** from 25 March 2020 for debts incurred in the ordinary course of business – see here. Despite that, companies will remain liable to pay any debts incurred and so you should take all reasonable steps to minimise or avoid your company incurring debts that you may not be able to pay.

Q: What about employees?

A: Be innovative and consult, both in terms of protecting your business now and into the future.

Whatever you do, you must act lawfully, and this will be guided by legislation as well as the terms of employment (whether under contract, collective agreements or underpinning awards).

Talk to your employees about the challenges and options. Matters you consider could include:

I. Closing one or more work locations and directing employees to stand down and stop work;

II. With an employee's agreement, reducing the employee's hours of work or remuneration;

III. With prior consultation, notifying employees of changes to their rosters, hours and other major workplace changes; and

IV. Ending the employment of employees on grounds of redundancy.

If an employee will agree to a reduction of hours, or pay, for a temporary period, that avoids any dispute. It may also mean you can keep more people employed for longer. When this ends (and it will) **you will need flexibility to scale up quickly**.

If you are considering a 'stand-down', this can be done under the *Fair Work Act 2009* (Cth). The Act allows employers to 'stand-down' employees without pay during a period in which the employee cannot usefully be employed because of a stoppage of work for any cause for which the employer cannot reasonably be held responsible. **Not every business can use the stand-down provisions**, and you should seek specific advice. Where working from home arrangements are in place (or can be in place) it becomes harder. Care should be taken, because getting it wrong might result in significant back-pay obligations and/or penalties.

Changes allowing greater flexibility in working arrangements or for access to entitlements continue to be developed. For example, in NSW changes have been made regarding the ability to access long service leave entitlements, and there are changes to awards being sought to allow more flexibility. As such, continuing to receive current advice remains critical to being aware of the options available and to making the right call.

Where an employee remains in the workplace, don't forget about the ongoing need to manage the risks of exposure. You can lawfully:

a. direct employees not to attend the workplace and to take leave if they present as a moderate-high risk of having COVID-19; and

b. give other reasonable and lawful directions to employees and others attending work so that the company and its workers can meet their work health and safety duties.

FAQs

Q: Is the $100,000 cash flow boost available to all small businesses, including sole traders and start-ups?

A: Unfortunately, many small businesses, including start-ups and sole traders, do not benefit greatly from the specific tax concessions announced in the Federal Government's stimulus package. You can read about all of these measures in more detail on the ATO's website here.

The critical concessions are aimed either at **rates of depreciation** or **write off of equipment**, or **employment related tax liabilities**, specifically:

I. Federal Government Pay as You Go (Withholding) – *PAYG(W)* – which is the tax withheld from employees' wages; and

II. State Government payroll taxes – which are additional taxes paid on employees' wages and contractor payments, over various thresholds in each State, which are well in excess of the wages bill of most start-ups and smaller businesses.

The PAYG(W) refund has received a lot of coverage because it **allows for a payment to eligible small businesses of up to $100,000**.

This payment (called a "cash flow boost") applies where **a small business pays wages to employees**. It is equal to the amount reported in quarterly or monthly business activity statements from March, and even if the amount withheld is relatively small (or zero) there will be a minimum payment of $10,000.

The payment is tax free, never has to be repaid, and the PAYG(W) amount reported on the BAS is still deductible.

It is a very generous concession for small businesses with employees, however, for sole traders and start-ups who do not have employees (or do not make voluntary withholding payments in relation to contractors) there is no benefit at all. This seems particularly unfair, as sole traders still pay tax on their taxable income, and quite often need the cash flow boost desperately.

The legislation also introduced specific **anti-avoidance provisions** to prevent small businesses restructuring their employment arrangements so as to artificially take advantage of the cash flow boost, for example, by paying large bonuses to staff who are family members. The ATO will no doubt use its extensive data matching and audit powers to identify businesses that it perceives are taking advantage of this concession.

Q: Is there any other way to pay less tax, or receive a refund of my tax?

A: Beyond these measures, the ATO has announced a range of options that may be available on a **case-by-case basis to defer tax liabilities and reduce penalties and interest**. This announcement is welcome (particularly the reduction of penalties and interest), however it does not remove the liability for tax completely.

It is possible to vary instalment notices (the pre-payment of the current year's income tax based on an estimate from previous years), however, this has always been possible if circumstances change. This can temporarily ease the tax cash flow burden on businesses (and can even allow a refund to apply for previous periods), but it will not change the final tax liability when tax returns are lodged at year's end.

Answer continued overleaf…

FAQs

Currently, the ATO is granting a six month deferral on any outstanding tax liabilities. Note that this is only a deferral, and while it is expected that the ATO will continue to show some flexibility at the end of this period, past experience from events such as 11 September 2001, the GFC and natural disasters shows that their patience will not be unlimited. Businesses that defer their tax liabilities should have a clear plan in place to clear the outstanding tax liability within a reasonable time when the deferral period comes to an end.

It is critical to continue to lodge your returns and statements on time, as penalties can still apply for late lodgment. Further, non-lodgment is a ground for refusal of future payment plans (for example, at the end of the six month deferral period). For those businesses that operate as companies, failure to lodge by the due date can also lead to inescapable personal liability for directors.

Q: Will the Government introduce measures that can actually provide my business with permanent assistance?

A: Understandably, and laudably, the Government released the above measures quickly, without extensive consultation, and with the aim of benefiting as many small businesses as possible. It is also worth noting that the Federal Government appears to have recognised that the measures, as initially released, will have unintended consequences and gaps. Treasury has established a *Coronavirus Business Liaison Unit* to help bridge any gaps and potentially provide additional support to those businesses which miss out. Submissions to this body may be a helpful way to provide cash flow support more equitably to sole traders, start-ups and other small business operators who do not yet benefit from the most significant concessions.

Q: What can be done if I have a corporate transaction afoot?

A: You may wish to consider your rights under the applicable transaction documents, including if a material adverse change (MAC) clause has been triggered, which may give rights to terminate the contract (if you no longer wish to proceed, or if the other party no longer wishes to proceed). Also, keep in mind any commitments you have given under such documents (such as warranties or indemnities relating to your business), and if those commitments can still be given in the circumstances.

Q: What about shareholder and investor meetings?

A: If you have a shareholder or investor meeting coming up, think about the format, such as the ability for it to be held virtually (and check your company constitution or other governing documents to ensure that you are holding a valid meeting). ASIC has also given guidance on holding meetings currently - see here.

Q: What should I do about investors?

A: Even without a meeting, don't forget your investors. While the current environment may not be ideal for capital raising activities, remember to keep an eye on your runway and remember that a capital raising can take between 3 to 9 months, from initial discussions with investors, to term sheet, to finalisation of the investment. Keep in touch with your existing investors and supporters – you never know what support they might be able to provide (and when) – and continue to keep future potential investors and supporters warm and aware of your activities. If you were thinking about a crowd funding campaign, continue to keep thinking about communicating with, and growing, your crowd – the 'community' aspect of a crowd funding campaign may well be a viable source of funding in the coming months.

Lawyers | McCullough Robertson

DATA SECURITY - CHECKLIST

Ensuring business continuity in the time of the COVID-19 pandemic: Data security risks

As Governments implement severe measures to fight the COVID-19 pandemic, businesses are increasingly reliant on remote Internet-connected workforces in order to ensure business continuity. With this shift to remote working, comes heightened data sensitivity risks, including **an increase in the likelihood of cyber attacks and privacy breaches**.

Businesses must be vigilant of this heightened risk environment. Despite the extraordinary environment in which we find ourselves, data security and privacy obligations continue to apply.

This means that you should:

Get your remote security measures in place

- ❑ evaluate all SaaS applications that your staff use while remote working to ensure adequate levels of protection and security;
- ❑ ensure your systems capacity is adequate given the increased usage;
- ❑ ensure adequate encryption levels are applied to the data at rest and in transit;
- ❑ implement virtual private networks and multi-factor authentication measures;
- ❑ undertake data back-ups regularly to prevent against data loss;
- ❑ maintain logs of equipment being used by staff at home;
- ❑ provide information security refreshers to your staff working from home;
- ❑ insist that staff only communicate through your official systems, not through publicly-available social media channels; and
- ❑ remind staff of their confidentiality obligations, including the need to store and dispose of hard-copy records securely.

Carefully manage your suppliers that have access to your data

- ❑ get sufficient comfort that the IT controls that your suppliers implement work and that they are effective in terms of protecting your data;
- ❑ manage contractual liability with your suppliers around cyber incident and data breach issues – this includes having clear protocols in your contractual arrangements which deal with:
    - the communication of suspected breaches by your supplier;
    - the processes for conducting assessments into those breaches; and
    - the allocation of responsibility for the containment, remediation and notification of the breach; and
- ❑ ensure that you control any notifications to your customers and any regulators, including the Office of the Australian Information Commissioner (OAIC) – this will help to manage any reputational fall-out.

Lawyers | McCullough Robertson

DATA SECURITY – CHECKLIST

Know what do in the event you are hacked

- ❑ have your crisis management team ready for immediate mobilisation and response – a team of multi-disciplinary specialists (including, as appropriate, IT, legal, risk and compliance, PR/communications, corporate affairs, HR) which is known in advance and has full authority to act without permission;
- ❑ ensure you have a robust data breach response plan which can be implemented immediately – a plan which sets out:
    - your strategy for containing, assessing and managing a data breach from start to finish - with clear reporting lines, escalation paths and criteria for when to mobilise the crisis management team;
    - your strategy for dealing with the communication of the data breach internally and externally - including to affected individuals, the OAIC and other regulators that may be relevant to your business;
    - the roles and responsibilities of staff members; and
    - processes for dealing with a data breach involving another entity, such as your IT supplier;
- ❑ make sure you get the facts of the data breach – don't just rely on assumptions;
- ❑ carefully manage communications to internal and external stakeholders – including setting the correct narrative for the data breach and your response from the outset;
- ❑ build a stakeholder map, and consider the legal relationship you have with each stakeholder so as to ultimately guide you to a prioritised work plan for responding to the incident;
- ❑ seek the protection that can be gained through legal professional privilege by engaging with your internal or external legal advisers – otherwise sensitive internal communications and documents about the breach (including forensics reports) could be exposed to regulators or those pursuing civil damages claims against you;
- ❑ determine your notification obligations at law – to affected individuals, to the OAIC and to any other regulators relevant to your business – see below for further details; and
- ❑ consider your contracts that may be impacted by the cyber incident, including rights and obligations that may be triggered.

Lawyers | McCullough Robertson

DATA SECURITY – CHECKLIST

Comply with your legal obligations to report privacy breaches

You have **obligations under the *Privacy Act 1988* (Cth) to report certain data breaches** (known as "eligible data breaches") if you are a:

I. Commonwealth Government agency;

II. Private sector organisation (including not-for-profit) with annual turnover in excess of $3 million; or

III. A small business earning $3 million or less that provides health services, is involved in trading in personal information, provides services under a Commonwealth contract or a credit reporting body.

An "eligible data breach" occurs if:

I. There is unauthorised access to, or disclosure of, information, or information is lost in circumstances where such unauthorised access or disclosure is likely to occur;

II. A reasonable person would conclude that access or disclosure would be likely to result in "serious harm" to any of the individuals to whom that information relates; and

III. You have not been able to prevent the likely risk of serious harm with remedial action.

Assess

In the case of a suspected data breach, you **must undertake a reasonable and expeditious assessment** (and, in any event, within 30 days) to determine whether there are reasonable grounds to believe that an "eligible data breach" has occurred.

Notify

If you have reasonable grounds to believe that an "eligible data breach" has occurred, you must as soon as practicable:

- ❑ prepare a statement setting out:
  - your contact details;
  - a description of the data breach;
  - the kinds of information concerned; and
  - the steps you recommend individuals take to mitigate the harm that may arise from the data breach;
- ❑ give a copy of the statement to the OAIC; and
- ❑ take such steps as are reasonable in the circumstances to notify affected individuals of the contents of the statement.

Lawyers | McCullough Robertson

DATA SECURITY – CHECKLIST

Serious harm?

The key test for notification is whether the actual or suspected data breach is "likely to result in serious harm" to individuals.

You should have regard to the following, among other relevant matters, when assessing whether individuals are likely to suffer "serious harm":

- the kind and sensitivity of the information involved in the breach;
- whether the information is protected by security measures(s) and the likelihood of overcoming that protection;
- the persons, or kinds of persons who have obtained, or could obtain, the information;
- if a security technology or methodology was used to make the information unintelligible or meaningless – the information or knowledge that would be required to circumvent the technology or methodology; and
- the nature of the harm – whether that harm be physical, psychological, emotional, reputational, economic or financial.

It is not just the likelihood of the harm occurring, but also the anticipated consequences for individuals if the harm was to materialise (e.g. risk of identity theft).

As the notifiable data breaches scheme is relatively new, the meaning of "serious harm" is still somewhat nebulous. From a reputational perspective, it is often best err on the side of caution and to make the required notifications if there is doubt as to whether the threshold of "serious harm" has been reached.

Penalties

A failure to notify an "eligible data breach" is considered an interference with the privacy of an individual affected by the breach. Serious or repeated interferences with the privacy of an individual can give rise to civil penalties of up to $2.1 million.

McCullough Robertson Lawyers

LEASING IN PRECARIOUS TIMES (TENANT)

During these precarious times, tenants should be aware of a number of risk management measures that can be implemented to mitigate the impact of the COVID-19 pandemic on their leasing arrangements.

Measures to mitigate risk

Given each lease is usually subject to bespoke negotiations, it is **important the terms of each individual lease are reviewed**. Below are some risk management measures tenants can implement to mitigate the impact of COVID-19:

I. Review insurance policies to ensure business disruption is recoverable (including obtaining crisis management insurance);

II. Engage in discussions with landlords if paying rent becomes difficult. Some options include:

- entering a moratorium to delay the payment of rent;
- requesting a rent free period in exchange for agreement to extend the term of the lease by a period equal to the rent free requested; or
- requesting a temporary conversion to turn-over rent.

III. Review incentive arrangements to ensure that closure of the building which amounts to a breach does not result in forfeiture of any incentive; and

IV. If new leases are being negotiated or leases extended, request a force majeure clause be inserted which includes public health pandemics.

Can you stop trading?

Payment of rent is an essential term under any lease. In the absence of an express provision allowing a tenant to cease trading in the event of a disease pandemic, it is unlikely tenants can simply stop trading or paying rent during any closure period. Accordingly, **a tenant's decision (without the landlord's approval) to close the premises could amount to a breach of the lease**.

Commercial leases do not necessarily contain a positive obligation on tenants to continue trading. In essence, provided the tenant keeps paying rent in accordance with the terms of the lease, there is no requirement to keep the premises open.

Rent reduction

Unless the lease contains a specific rent reduction clause, the tenant does not have grounds to request a rent reduction if the building is closed or access is restricted.

The **specific wording of the clauses in the lease should be reviewed** to ensure it covers a public health pandemic.

Whether the landlord takes the commercial view in the prevailing circumstances to reduce rent is at the landlord's sole discretion.

Force majeure

Some leases may contain a force majeure clause that relieves a party of its obligations if circumstances outside its control make it impossible to perform them.

Ultimately, the consequences of such a clause **depends on how the force majeure event is defined**. Terms such as 'pandemic' or 'disease' could cover COVID-19. Similarly, clauses referring to 'acts of government' or 'impacts from the exercise of governmental powers' could qualify as force majeure events and permit a party to the lease to be excused from performing their obligations under the lease.

If the lease does not contain a force majeure clause, it is unlikely that there are grounds for either party to be excused from their leasing obligations.

Changes in legislation

At the time of writing this article, NSW had passed legislation which gives NSW Ministers wide ranging powers in relation to leasing, including regulations to prevent landlords terminating leases. Further details are yet to be disclosed and the other States are expected to follow suit.

We recognise that things are moving quickly and we encourage you to keep following our updates as we will share further information when known.

Need help?

We are advising a number of organisations in relation to COVID-19 including its impact on their leasing arrangements. **If you would like us to give your lease a health check so you can better understand your rights and obligations during these precarious times, please contact us.**

For enquiries or assistance in relation to any of the material contained within this guide, please contact one of our key contacts overleaf.

Lawyers | McCullough Robertson

CONTACT CARD

Scott Butler
Partner - Insolvency
P: +61 448 939 439
E: sbutler@mccullough.com.au

Cameron Dean
Partner - Employment
P: +61 407 407 032
E: cdean@mccullough.com.au

Matt (Matthew) McMillan
Partner – Data Security
P: +61 437 571 910
E: mmcmillan@mccullough.com.au

David Hughes
Partner – Tax
P: +61 419 773 415
E: dhughes@mccullough.com.au

Kristan Conlon
Partner – Real Estate
P: +61 421 613 076
E: kconlon@mccullough.com.au

Ben Wood
Partner - Corporate
P: +61 416 820 423
E: bwood@mccullough.com.au

Jason Munstermann
Partner - Litigation
P: +61 418 482 717
E: jmunstermann@mccullough.com.au

Eva Vicic
Partner – Real Estate
P: +61 421 895 314
E: evicic@mccullough.com.au

Brett Sangster
Partner - Commercial
P: +61 419 339 264
E: bsangster@mccullough.com.au