Williamson Chaseling
Accounting & Financial Services
Phone 02 4926 4233
Email wcpl@willchase.com.au

New data breach laws come into effect

New data breach rules in effect from 22 February 2018 place an onus on business to protect and notify individuals whose personal information is involved in a data breach that is likely to result in serious harm.

In October last year, almost 50,000 employee records from Australian Government agencies, banks and a utility were exposed and compromised because of a misconfigured cloud based 'Amazon S3 bucket'. AMP was reportedly one of the worst affected with 25,000 leaked employee records. ITNews reports that the data breach was discovered by a Polish researcher who conducted a search for Amazon S3 buckets set to open, with "dev", "stage", or "prod" in the domain name. One contractor appears to be behind the breach.

In October 2016, the details of over half a million Red Cross blood donors were inadvertently exposed after a website contractor created an insecure data backup. In the US, a massive data breach exposed the credit records (including social security records) of over 145 million Americans – all because an IT worker didn't open an email about a critical patch for their software.

Regardless of how good your existing systems are, data breaches are a reality either through human error, mischief, or simply because those looking for ways to disrupt are often one step ahead. But it's not all about IT, there have been numerous cases of hard copy records being disposed of inappropriately, employees allowing viruses to penetrate servers after opening the wrong email, and sensitive data on USBs lost on the way home.

Who is covered by the data breach scheme?

The Notifiable Data Breach (NDB) Scheme affects organisations covered by the Privacy Act - that is, organisations with an annual turnover of $3 million or more. But, if your business is 'related to' another business covered by the Privacy Act, deals with health records (including gyms, child care centres, natural health providers, etc.,), or a credit provider etc., then your business is also affected. Special responsibilities also exist for the handling of tax file numbers, credit information and information contained on the Personal Property Securities Register.

What you need to do

It's important to keep in mind that complying with these new laws means more than notifying your database when something goes wrong. Organisations are required to take all reasonable steps to prevent a breach occurring in the first place, put in place the systems and procedures to identify and assess a breach, and issue a notification if a breach is likely to cause 'serious harm'.

Taking all reasonable steps – assessing risk

The Privacy Act already requires organisations to take all reasonable steps to protect personal information. The new data breach laws merely add an additional layer to assess breaches and notify where the breach poses a threat. For example, if you have not already, you should assess issues such as:

- How personal information flows into and out of your business. For example:
  - What information do you gather (including IP data from websites)
  - What information do you provide (for example, do you provide information on your clients to third parties?)

    - Where private information is stored – map out what systems you use, where these systems store data (if cloud based, your data may be held in a foreign country), what level of security is provided within those systems, and what level of access each team member has (and what they should have access to for their role)
- How private information is handled by your business across its lifecycle and who has access at each stage (not just who is accessing the information for their work but who 'could' access this information)
- Possible impacts on an individuals' privacy (risk assessment)
- The policies and procedures in place to manage private information, including risk management and mitigation, whether these are adhered to, and actively managed
- The policy review process - review policies and procedures at least annually but again with the introduction of new systems and technology. Remember, you can't just have a policy sitting somewhere, it needs to be actively reinforced and adopted by team members
- Instate new project protocols for ensuring privacy where personal information is at risk
- Document everything including your reviews and procedural updates even if nothing changed. If there is ever an issue where your business's culpability is assessed, your capacity to prove that you took all reasonable steps will be important.

When it comes to data breaches, all organisations must have a data breach response plan. The data breach plan covers the:

- Actions to be taken if a breach is suspected, discovered or reported by a staff member, including when it is to be escalated to the response team
- Members of your data breach response team (response team), and
- Actions the response team is expected to take.

The Office of the Australian Information Commissioner provides a sample breach response plan.

Identifying a serious breach

So, what is a serious breach? A breach has occurred when there is unauthorised access to or disclosure of personal information or a loss of personal information that your business holds. Whether a breach is serious is subjective but may include serious physical, psychological, emotional, financial, or reputational harm. If a breach occurs, you need to think through how that information could be used for identity theft, financial loss, threats to physical safety (for example someone's home address), job loss, humiliation or reputational damage, or workplace bullying or marginalisation.

If you suspect a breach has occurred, your business is obliged to take "reasonable" and "expeditious" action regardless of whether you think it is serious or not (under the NDB scheme you have a maximum of 30 days to assess the damage and respond but in general, the first 24 hours is often crucial to the success of your response). Ignorance is not a defence. A lack of systems to identify system breaches fails the Privacy Act's requirement to take all reasonable steps to protect personal information. As soon as a breach is identified anywhere in the business, whether it is IT based or physical, steps need to be taken - even if it is simply noting that no further action is required.

If you suspect a data breach has occurred that may meet the threshold of 'likely to result in serious harm', you must conduct an assessment. Sounds simple right? But the problem for business is often that there are initially no definitive answers about the extent of a breach or its seriousness for the assessment to take place. Take the example of a retail business with an online store. A hacker exploiting an unpatched vulnerability in your customer relationship management (CRM) system gains access to the customer database for your online store,

which includes customer purchase histories and contact details. IT calls you and tells you there is a problem but can't tell you how, what customer records are affected, and if the records have been compromised. You don't want to scare your customers by advising of a breach but you don't the impact yet. What do you do? The first step is generally to contain the damage - isolate or shutdown the affected system to prevent further potential loss - then assess the scenario quickly – not just because of the NDB scheme but because your business's reputation is on the line.

Notifying a breach
If a breach is assessed to potentially result in serious harm, you are obliged to advise affected individuals and the Australian Information Commissioner. You have the option to:

- Notify all individuals whose personal information is involved in the eligible data breach
- Notify only the individuals who are at likely risk of serious harm; or
- Publish your notification, and publicise it with the aim of bringing it to the attention of all individuals at likely risk of serious harm.

You advise the Australian Information Commissioner of a serious potential breach using the Notifiable Data Breach statement.

And it's not just Australia. Does your business have international connections?
Data breaches are common and many countries have moved to ensure that the personal information of individuals is protected. If your business operates overseas or has customers overseas you need to be aware of the requirements in those countries.

Most US states have compulsory data breach requirements. The European Union's General Data Protection Regulation (GDPR) comes into effect from 25 May 2018. If you operate through a local distributor in the European Union or have direct supply into those countries then it's likely your business will be caught by the Regulation.

Directors on 'hit list' for not paying employee super

Proposed legislation would see the ATO pursue criminal charges against Directors who fail to meet their superannuation guarantee (SG) obligations.

An analysis by Industry Super Australia submitted to the Economics References Committee into *Wage Theft and Superannuation Guarantee Non-compliance*, indicates that employers failed to pay an aggregate amount of $5.6 billion in SG contributions in 2013-14. On average, that represents 2.76 million affected employees, with an average amount of over $2,000 lost per person in a single year. The ATO's own risk assessments suggest that between 11% and 20% of employers could be non-compliant with their SG obligations and that non-compliance is "endemic, especially in small businesses and industries where a large number of cash transactions and contracting arrangements occur."

At present, under reporting or non-payment of SG is usually discovered when the employer misses the quarterly payment schedule or from the ATO's hotline.

New legislation seeks to introduce a series of changes to how employers interact with the SG system and give some teeth to the ATO to pursue recalcitrant employers. The new rules, if passed by Parliament, generally come into effect from 1 July 2018.

The key changes include:

The ATO can force you to be educated about your SG obligations

At present, if an employer fails to meet their quarterly SG payment on time they need to pay the SG charge (SGC) and lodge a Superannuation Guarantee Statement. The SGC applies even if you pay the outstanding SG soon after the deadline. The SGC is particularly painful for employers because it is comprised of:

- The employee's superannuation guarantee shortfall amount – so, all of the SG owing
- Interest of 10% per annum, and
- An administration fee of $20 for each employee with a shortfall per quarter.

Unlike normal SG contributions, SGC amounts are not deductible, even if you pay the outstanding amount. That is, if you pay SG late, you can no longer deduct the SG amount even if you bring the payment up to date.

And, the calculation for SGC is different to how you calculate SG. The SGC is calculated using the employee's salary or wages rather than their ordinary time earnings. An employee's salary and wages may be higher than their ordinary time earnings particularly if you have workers who are paid for overtime.

Under the quarterly superannuation guarantee, the interest component will be calculated on an employer's quarterly shortfall amount from the first day of the relevant quarter to the date when the SG charge would be payable.

Where attempts have failed to recover SG from the employer, the directors of a company automatically become personally liable for a penalty equal to the unpaid amount.

Under the proposed rules, the ATO will also have the ability to issue directions to an employer who fails to comply with their obligations. The Commissioner can direct an employer to undertake an approved course relating to their SG obligations where the Commissioner reasonably believes there has been a failure by the employer to comply with their SG obligations, and, of course, a direction to pay unpaid and overdue liabilities within a certain timeframe.

Criminal penalties for failure to comply with a direction to pay

Employers who fail to comply with a directive from the Commissioner to pay an outstanding SG liability face fines and up to 12 months in prison. Before hauling anyone off to prison the ATO has to consider the severity of the contravention including:

- The employer's history of compliance (superannuation and general tax obligations)
- The amount of unpaid super relative to the employer's size
- And steps taken by the employer to pay the liability, and
- Any matters the "Commissioner considers relevant".

The ATO will tell employees if an employer is under paying or not paying SG

The proposed new rules will allow the ATO to tell current and former employees about the failure (or suspected failure) of an employer to comply with their SG obligations. The ATO can also advise the employees what action has been taken by the ATO to recover their SG.

This disclosure cannot relate to the general financial affairs of the employer.

Extension of Single Touch Payroll to all employers
Single Touch Payroll – the direct reporting of salary and wages, PAYG withholding and superannuation contribution information to the ATO – will be compulsory from 1 July 2018 for employers with 20 or more employees. Under the proposed rules, this system would be extended to all employers by 1 July 2019.

In addition, Single Touch Reporting will extend to the reporting of salary scarified amounts.

What's changing in 2018?

1 January 2018

- **Vacancy fees for foreign acquisitions of residential land** - An annual vacancy fee imposed on foreign owners of residential real estate if the property is not occupied or genuinely available on the rental market for at least 183 days in a particular 12 month period. Foreign owners can avoid the fee by living in the property (or have a family member live in the property), leasing the property, or making it available for rent, for a total of 183 days in a 12 month period. Short term letting arrangements often won't be sufficient to avoid the levy.
- **CGT concession for investments in affordable housing** - The CGT discount will be increased for individuals who choose to invest in affordable housing. The current 50% discount will increase by 10% to 60% for resident individuals who elect to invest in qualifying affordable housing. Non-residents are not generally eligible for the CGT discount. *This change is not yet legislated.*

1 July 2018

- **Super concessions for downsizers come into effect** - If you are over 65, have held your home for 10 years or more and are looking to sell, you can contribute a lump sum of up to $300,000 per person to superannuation without being restricted by the existing non-concessional contribution caps - $100,000 subject to your total superannuation balance - or age restrictions.
- **Using super to save for your first home** - The first home savers scheme will enable first-home buyers to save for a deposit inside their superannuation account, attracting the tax incentives and some of the earnings benefits of superannuation. Home savers can make voluntary concessional contributions (for example by salary sacrificing) or non-concessional contributions (voluntary after-tax contributions) of $15,000 a year within existing caps, up to a total of $30,000. When you are ready to buy a house, you can withdraw those contributions along with any deemed earnings in order to help fund a deposit on your first home.
- **GST on low value imported goods -** GST will apply to retail sales of low value physical goods ($1,000 or less) that have been imported into Australia and sold to consumers.
- **Who pays the GST on residential property & subdivisions -** Property developers will no longer manage the GST on sales of newly constructed residential properties or new subdivisions. Instead, the Government will require purchasers to remit the GST directly to the ATO as part of the settlement process. *This change is not yet legislated.*

- **$20k immediate deductions ends** – The $20,000 immediate deduction threshold for assets purchased by businesses with an aggregated turnover of under $10 million ends 30 June 2018.
- **Taxable payments reporting system extended to couriers & cleaners** - Businesses in the courier and cleaning industries will need to collect information from 1 July 2018, with the first annual report required to be lodged in August 2019.
- **Single Touch Payroll –** Single Touch Payroll reporting starts for employers with 20 or more employees. Employers will report payments such as salaries and wages, PAYG withholding and super information directly to the ATO from their payroll system at the same time they pay their employees.
- **Closing salary sacrifice loopholes to reduce super guarantee -** Loopholes that enable employers to reduce the Superannuation Guarantee (SG) contributions owed to employees by using salary sacrifice contributions will be closed. *This change is not yet legislated.*
- **Access to reduced company tax rate limited** - Limits access to the 27.5% company tax rate by replacing the existing 'carrying on a business test' with a passive income test. Under the new rules, a company will not be able to access the reduced company tax rate if more than 80% its assessable income is passive in nature. *This change is not yet legislated.*
- **Wine equalisation tax rebate tightened eligibility -** Wine producers will be required to own at least 85% of the grapes used to make the wine throughout the winemaking process and brand wine with a trademark.

Quote of the month

"When you reach the end of your rope, tie a knot in it and hang on."
Franklin D. Roosevelt