ACCOUNTANTS & AUDITORS

With Compliments

The POPIA (The Protection of Personal Information Act) compliance deadline is 30 June 2021. If you have not yet attended to the development of a POPIA implementation and compliance framework to ensure that your business complies with POPIA, you should act now.

Every business is unique in its functioning and operations and therefore has different needs when it comes to POPIA implementation. With this in mind, we are able to refer you to an alliance partner who has assisted us with our own tailored POPIA implementation.

Regards

Alexis and Dave

MD House
Greenford Office Estate
Off Punters Way
KENILWORTH
7708

Tel: 021 683 4834
Fax: 086 541 2872
Email: newsletters@mdacc.co.za
Website: www.mdacc.co.za

CA(SA) CHARTERED ACCOUNTANT SOUTH AFRICA

In this Issue

Subscribe

May 2021

Uncertain, Costly Power Supply: How to Mitigate Your Risk

"The more that energy costs, the less economic activity there can be" (Robert Zubrin)

It has been 13 long years since we first experienced load shedding in 2007. Since then, businesses have lost thousands of hours of productivity and significant amounts of money to these "rolling blackouts".

The situation is not going to improve – more load shedding is predicted, by Eskom itself, for the next five years together with even higher electricity tariffs. Given the impact of load shedding and the high cost of electricity, business owners are well-advised to understand and assess the risks faced in terms of electricity supply and to implement strategies to mitigate this risk.

Impact on companies

In addition to its devastating impact on the economic environment in which companies operate, all businesses that use electricity for machinery, technology and light, experience a loss of production during power outages - even those with backup batteries or generators.

Smaller and medium sized businesses that cannot afford alternative energy solutions are disproportionately disadvantaged. Unable to provide any service, they lose customers too.

Companies also suffer physical damages from load shedding, for example, to computers and other electronic equipment, perishables damaged in refrigerators and raw materials wasted as production cycles are interrupted, and the inability to deliver to clients as load shedding affects traffic flow.

During load shedding, companies are also exposed to a greater security risk, as well as a theft and burglary risk, as security systems and processes are compromised, which, in addition, could affect their insurance cover.

Six ways to mitigate your electricity risk

1. **Stay abreast**. Task a team member to stay up-to-date with, for example, a load shedding notification app. This will ensure better planning, so the time when there is power can be maximised. It will also enable staff to minimise damage to equipment by switching off correctly before load shedding commences and to reduce stress by ensuring data is backed up.

2. **What is measured is managed**. A professional energy audit for your business will allow you to understand your energy needs and usage patterns. This is the first step to finding the right alternative that may simplify and optimise power usage, lower costs and improve business performance.

3. **Consider alternative energy solutions**, ranging from simple uninterruptible power source (UPS) units and back-up solutions to small or large battery-based and generator solutions, to a variety of solar PV (photovoltaic) solutions. While the initial cost of converting to solar power or purchasing a generator may seem high, the consequential costs of Eskom's uncertain supply and fast-rising tariffs are also mounting. The cost of solar power equipment, for example, has decreased significantly, making it possible to generate power at a cost lower than the national grid. (This may well be a viable solution particularly if your business operates mainly during daylight/sunlight hours).

4. **Explore financing options for funding.** The impact of the initial capital outlay for alternative energy solutions can be reduced with the right finance. The alternative energy solutions division at FNB Business for example says it has seen a significant increase in demand for funding for renewable energy solutions, with solar PV being the most popular, and are projecting a significant increase in alternative energy funded solutions by the end of the year.

5. **Find out what incentives your company might benefit from**. For example, Eskom is planning to test a “critical peak pricing” pilot tariff with qualifying large customers.

6. **Another example is Section 12B of the Income Tax Act**, which provides for a capital allowance for movable assets used in the production of renewable energy and incentivises the development of smaller solar PV energy projects with an accelerated capital allowance of 100% in the first year for solar PV energy of less than 1MW.

   The companies tax rate in South-Africa is 28%. With this incentive, the value of a new solar power system may be deducted as a depreciation expense from the company’s profits. This means that the company’s income tax liability will be decreased by the same value as the value of the installed solar system. This reduction can also be carried over to the next financial year as a deferred tax asset. **This is a direct saving of 28% on the purchase price from day one on the solar system!**

A Basic Guide to PAYE and Four Common Mistakes

“The point to remember is that what the government gives it must first take away” John S. Coleman

If it weren't for the PAYE system, which forces employees to pay taxes as they earn their money, each of us would be liable for a lump sum payment of between 18% and 45% of our total monthly earnings at the end of each tax year. Pay As You Earn (PAYE) requires that employers deduct money from their employees’ earnings as they earn it, and pay this money over to SARS on the employees’ behalf.

The Basics

To calculate PAYE an employer should multiply an employee’s taxable earnings (which include any fringe benefits such as Disability Benefit Contributions etc.) by 52 weeks, 26 weeks or 12 months (depending on how often they get paid) to get an annual amount. This annual sum is then cross-referenced against the SARS tax tables to calculate annual tax. This is then divided again by the same work period to get the monthly PAYE tax which is then withheld, displayed on your IRP5 and paid over to SARS.

Example

1. Regular monthly income = R10,000.
2. Annual equivalent = R10,000 x 12 = R120,000.
3. Tax **calculated** on R120,000 as per tax tables = R5,886.
4. **PAYE** payable on regular monthly income = R5,886/12 = R490.50 p.m.

In cases where an employer pays certain things like medical aid, pension fund, income protection and/or retirement annuity fund contributions on an employee’s behalf, the

employer must deduct these costs from the employee's earnings and take these deductions/credits into account when calculating PAYE and making payment to SARS. This is where problems begin to creep into the system.

Four Common Problems

1. **Travel Costs**

   Travel costs are a common area of concern for SARS as they can be miscalculated extremely easily. To determine the portion of the travel allowance that should be included in the calculation of an employee's taxable income, so as to determine the PAYE, the employer is required to implement an 80/20 rule. Either 80% of their mileage is for business purposes, and the remaining 20% of the allowance is subject to tax. Or, only 20% of their travel is business related, and the remaining 80% of the allowance must be taxed. To determine the percentage to be included in taxable income, accurate logbooks must be provided by employees so that the appropriate 80/20 rule can be strictly adhered to.
   Choosing the wrong rate here can expose an employee to substantially more tax than they should be paying.

2. **Disability Benefit Contributions**

   Prior to 1 March 2015 Disability Benefit Contributions could be deducted tax free from an employee's salary thereby reducing their PAYE contribution. Tax was then charged on the pay-out that the employee received in the event of a disability. This changed in March of that year, however, and now the Disability Benefit Contributions are no longer tax deductible and must be counted as being part of the employee's fringe benefits. The final Disability pay-outs are, fortunately, tax free.

3. **Retirement payments**

   Retirement payments give rise to another common error in the calculation of PAYE, mainly due to the fact that people are unaware that the system changed, and they are still implementing the old system. As of 1 March 2016, SARS now considers all company contributions to an employee's retirement and risk benefits as a fringe benefit which should be taxed.

   There are, however, instances in which a pension fund contribution may be tax deductible. This depends primarily on whether the pension fund is "approved" or "unapproved". Whether a retirement benefit is "approved" or "unapproved" is determined by the way its associated fund is administered as well as the rules of the fund. The broker who administers the fund will be able to tell you whether it is approved or unapproved and it will then be easier to work out just how to treat those deductions for PAYE.

4. **Partial tax year**

   Because PAYE taxes are calculated on a projected annual earning, those employees who work only part of a year are liable to benefit from a rebate. Effectively a person earning R30 000 a month would pay monthly PAYE based on an annual earning of R360 000 a year. If they only work for six months of that tax year they should then have only been charged for an annual tax earning of R180 000 and will be deserving of a rebate for the six months where they paid too much.

Speak to your accountant for detailed advice.

POPIA and Your Business: A Practical 5-Step Action Plan to Implement Now

"By failing to prepare you are preparing to fail" (Benjamin Franklin)

The media is awash with warnings about the dangers of not complying with POPIA (the Protection of Personal Information Act) by 1 July 2021, and indeed the risks of non-compliance are substantial.

The clock is ticking …. if anyone in your business needs to be motivated to take this seriously, refer them to the Countdown Clock on the Information Regulator's **website**.

Although you still have until the end of June 2021 to become fully compliant, **there are major benefits to understanding POPIA and starting the compliance process now - before it becomes compulsory.** The penalties for getting it wrong are sizeable, "preparation makes perfect", you are giving yourself time to get it right, and for many businesses there is also good marketing potential in being able to tell your customers and clients that you are already addressing the situation.

Five practical steps to start with…

Before we start on your action plan, **get to grips with the fact that you will almost certainly have to comply fully with POPIA.** As soon as you in any way "process" (collect, use, manage, store, share, destroy and the like) any personal information relating to a "data subject" (customers, members, employees and so on), you are a "responsible party". Very few businesses will fall outside that net. Equally you are unlikely to fall under exemptions like that applying to information processed "in the course of a purely personal or household activity". Get going with these steps -

1. **Information Officer:** Identify an "Information Officer" who will be responsible (and liable) for all compliance duties, working with the Regulator, establishing procedures, and training your team in awareness and compliance. You are automatically your business' Information Officer if you are its "Head" i.e. a sole trader, any partner in a partnership, or (in respect of a "juristic person" such as a company) the CEO, MD or "equivalent officer". You, your partnership or your company can "duly authorise" another person in the business (management level or above) to act as Information Officer and you can designate one or more employees (again management level or above) as "Deputy Information Officers". You will need to register both Information Officers and Deputy Information Officers with the Regulator, which (at date of writing)) says on its website that it is experiencing a technical glitch with its online registration portal but is working to resolve the issue – otherwise download the manual Registration Form **here**.

2. **Assess what personal information you hold, how you hold it, and why:** Figure out what personal information you currently hold, how you hold it, and why you hold it. To collect and "process" such information lawfully you need to be able to show that you are acting lawfully, reasonably in a manner that doesn't infringe the data subject's privacy, and safely.

   You must show that "given the purpose for which it is processed, it is adequate, relevant and not excessive", data can only be collected for a specific purpose related to your business activities and can only be retained so long as you legitimately need to or are allowed to keep it.

   There's a lot more detail in POPIA, but you get the picture – you cannot collect or hold personal information without good and lawful cause.

3. **Check security measures, know what to do about breaches:** You must "secure the integrity and confidentiality of personal information in [your] possession or under [your] control by taking appropriate, reasonable technical and organisational measures to prevent … loss of, damage to or unauthorised destruction of personal information … and unlawful access to or processing of personal information." You are going to have big problems if there is any form of breach from a risk that is "reasonably foreseeable" unless you can prove that you took steps to "establish and maintain appropriate safeguards" against those risks. Bear in mind that whilst cyber-attacks tend to get the most media time, there are also other risks out there – **brainstorm with your team all possible vulnerabilities and patch them.**

   Any actual or suspected breaches (called "security compromises" in POPIA) must be reported "as soon as reasonably possible" to both the Information Regulator and the data subject/s involved.

   If third parties ("operators") hold or process any personal information for you, they must act with your authority, treat the information as confidential, and have in place all the above security measures.

4. **Check if you do any direct marketing:** Most businesses don't think of themselves as doing any "direct marketing", but the definition is wide and includes "any approach" to a data subject "for the direct or indirect purpose of … promoting or offering to supply, in the ordinary course of business, any goods or services to the data subject…". So for example just emailing or WhatsApping your customers about a new product or a special offer will put you firmly into that net.

   If your approach is by means of "any form of electronic communication, including automatic calling machines, facsimile machines, SMSs or e-mail", you must observe strict limits. Whilst you can as a general proposition market existing customers in respect of "similar products or services" (there are limits and recipients must be able to "opt-out" at any stage), potential new customers can only be marketed with their consent, i.e. on an "opt-in" basis.

5. **Get a start on procedures and training:** Cover how you will collect the data, process it, store it, for how long, for what purpose/s and so on. What consent forms do you need and when/how are they to be completed and stored?

   You are much less likely to have a POPIA problem if everyone in your business (and most importantly you!) understands what your procedures are and implements them as a matter of course. Make sure that no functions "fall between two stools" – assign individual compliance tasks to named staff members and make sure everyone understands who is to do what.

This is a complex topic and there is no substitute for tailored professional advice. What is set out above is of necessity no more than a simplified summary of a few practical highlights.

Where does Fairness Belong in Your Business and Why Should You Care?

Many decisions are made on the basis of careful research and considerations about a variety of issues. Not all these deliberations will necessarily turn out to be correct. That in itself does not place question marks over the leadership's execution of its responsibilities in terms of the Companies Act to act with due care,

skill and diligence or the King IV Report Principle 1 that they should lead ethically and effectively.

Trust

An entity, which has been run and managed in such a way as to build a reputation for ethics, integrity and reliability, will likely have a growing group of loyal customers and other stakeholders, based on trust.

The size of the entity concerned has no bearing on whether or not it is trusted. That is based entirely on the entity's consistent, trust-centred behaviour towards all its stakeholders.

What if things go wrong?

There will be times when a decision turns out to be wrong resulting in a service or product not being delivered on time or otherwise being deficient. The reasons may be beyond the control of management. However, such an event may have the potential to negatively impact stakeholders' trust.

The cause may be the result of a strategic decision by management to change the nature or make-up of a service or product. For example, by reducing the size or contents of a product without any communication to consumers so as to increase profit margins or to avoid a price increase. This, of course, is a completely different proposition as it is inherently dishonest and lacking in transparency and integrity, questioning the moral mindset of management. Another example would be price-fixing and collusion. Some years ago this was evident in the construction and food processing industries.

A third example could be a deliberate decision to undertake activities without recognising the potential of damage to the environment; getting environmentalists, conservationists (some of whom may be customers) up in arms, and let's not forget the reach and impact of social media.

What are the consequences?

In all examples there is a real likelihood of a loss of trust resulting in customers abandoning the entity. In the second set of examples, where there is real or perceived dishonest behaviour on the part of management there are likely to be fines/penalties (which there were in the cases of the construction and food processing industries). **However, the real damage may well be the loss of trust – which for a smaller business could be fatal.**

In the former case where the problem arose through a situation that was either not anticipated or due to a change of circumstances, the loss of trust is still possible but appropriate remedial action may avoid the destruction of trust.

Finally, in the last example, how the entity responds to the situation will determine the long-term consequences.

Can fairness make a difference?

Having said that, where an entity responds by treating customers fairly, putting right the problem as a matter of moral rectitude, trust is likely to be retained and may even be enhanced. This, of course, requires swift and transparent communication so that stakeholders are aware of the circumstances of both the issue and the entity's response to it.

Consider the Autumn 1982 response of Johnson & Johnson to the deaths of seven

people in Chicago who had taken its market leading, over-the-counter painkiller, Tylenol.

Throughout the crisis thousands of stories ran in U.S. newspapers together with hundreds of hours of national and local television coverage. A major potential trust breakdown for Johnson & Johnson, bearing in mind that Tylenol was the market leading paracetamol in the US and a substantial contributor to J&J's revenue and profits. After the crisis, J&J said that over 90 percent of the American population had heard the story within the first week of the crisis.

J&J, however, did not have a crisis management plan, unthinkable today, or is it? Do you have anything like it?

So the company's Chairman, James Burke, went back to the company's founding credo. This saw the business as having a moral responsibility to society beyond sales and profit. He formed a seven-member strategy team with two tasks: how do we protect people and how do we save this product and our reputation?

First of all they alerted consumers via all available channels of communication not to consume any type of Tylenol product. They halted production and advertising and ordered a nationwide withdrawal of the product. This cost the company millions of dollars, however, it received credit for putting public safety above profit.

The cornerstone of J&J's recovery, in priority order, was: People, Environment, Property and only then Finance. They restored trust by behaving fairly to the most important people, their stakeholders. J&J's Tylenol, accordingly, ultimately re-gained its market share.

This is an example where fairness retained trust. There is even the possibility, as occurred in this case, of the enhancement of trust when, after the event, it is seen that the promise of fairness has been honoured in full.

Trustworthy fairness

So, all in all, treating all stakeholders fairly is a moral approach to business which enhances relationships. Even in personal relationships, responding with fairness when trust is at risk, can save the relationship.

An investment in fairness as a matter of corporate value is as essential and generates as good returns as fundamental trustworthy behaviour.

"In conclusion, it is clear to me that Trust and fairness in the workplace are connected as they are in all of life. Trust defines how we as humans relate to one to another, while fairness is a practical mechanism for maximising the benefits of trust. The two work together, and we need them both to operate consistently at the heart of workplace activity. In other words, 'Trustworthy Fairness' provides a foundation for building meaningful and productive workplace life" (Jonathan Rens).

Your Tax Deadlines for May 2021

- 7 May – Monthly Pay-As-You-Earn (PAYE) submissions and payments
- 25 May - Value-Added Tax (VAT) manual submissions and payments

- 28 May - Excise Duty payments
- 31 May - Value-Added Tax (VAT) electronic submissions and payments
- 31 May - Corporate Income Tax (CIT) Provisional Tax Payments where applicable

---