SOUTH AFRICAN INSTITUTE OF PROFESSIONAL ACCOUNTANTS™

YOUR WEALTH

SAIPA Your Law : Volume 12 Issue 2, 13 February 2017

This newsletter

This newsletter overviews new relevant National laws up to **13 February 2017**. Log-in to www.gazette.co.za, peruse the list and follow the hyperlinks to laws that interest you.

Please note that **[words in bold brackets]** in www.gazette.co.za show proposed deletions, and underlined words in www.gazette.co.za show proposed insertions - this allows you to see current and planned requirements at the same time, and helps with giving context to changes/proposed changes.

Log-in details for SAIPA Members

SAIPA Technical will keep you up to date with these changes so login and read the SAIPA YOUR LAW. Please see the last page for log-in details. Please provide SAIPA with your membership number when updating your details.

Index

Financial

01. National Credit Act: Credit Life Insurance Regulations

The Credit Life Insurance Regulations will commence 9 August 2017, and only apply to credit agreements entered into on 9 August 2017 or thereafter.

The Regulations will, amongst others, prescribe:

(i) Maximum cost of credit life insurance per life insured;

(ii) Different amounts for different credit agreements, while introducing a new 'affordable housing mortgage agreements' category;

(iii) Minimum cover arrangements in the event of a death, disability, unemployment and/or inability to earn (where relevant);

***Note**: A cost for the risk of unemployment or inability to earn will be prohibited if the consumer is an unemployed person at the time of entering into the agreement, and a cost for the risk of occupational disability will be prohibited if the consumer is a pensioner at the time of entering into the agreement.*

(iv) A measure of allowable cover variation where the consumer is a person employed in the informal sector, or is self-employed (whether in the formal or informal sector);

(v) That a credit provider must be able to show that the credit life cost was determined with regard to actual associated risk and liabilities, if requested to do so by the National Credit Regulator;

(vi) That a credit provider must respect the right of a consumer to substitute a credit life insurance; and

(vii) Limited grounds for excluding or limiting cover, including limitations regarding unemployment or inability to earn cover where a person knew three months in advance that they would be retrenched.

***Note**: Any such exceptions and limitations must be explained to the consumer on the date that the credit agreement is entered into and at regular intervals thereafter. It is not immediately clear why there is a time limit for situations where a consumer knew they would become retrenched, other than for procedural and onus convenience.*

GN103 GG40606 / 9 February 2017 (Incorporated into the National Credit Act and Regulations)

Back to index

Information

02. Draft Cybercrimes and Cybersecurity Bill

The Draft Cybercrimes and Cybersecurity Bill (no comment period - left to Parliament to invite comments) proposes, amongst others:

Cybercrimes

It will be an offence to:

(i) **Unlawful access:** unlawfully and intentionally secure access to data, a computer program, a computer data storage medium or a computer system (System);

Note *that authorisation will be a key question - is the person lawfully entitled to access, does he or she have lawful consent of another to access, and does he or she not exceed his or her entitlement or consent.*

(ii) **Unlawful acquisition**: unlawfully and intentionally overcome any protection measure which is intended to prevent access to data and use, examine, copy, move or divert data;

Note *that having data to which there is a reasonable suspicion that it was acquired unlawfully and not being able to give a satisfactory exculpatory account of such possession will also be an offence.*

(iii) **Unlawful interference I**: unlawfully and intentionally interfere (delete, alter, render ineffective, interrupt, deny access) with data or a computer program;

(iv) **Unlawful interference II**: unlawfully and intentionally interfere with a computer data storage medium or a computer system;

Note *that interference includes permanently or temporarily altering any resource or interrupting or impairing the functioning, confidentiality or integrity.*

(v) **Unlawful login**: unlawfully and intentionally acquire, possess, provide or use a password, an access code or similar data or device to commit a cybercrime;

Note *that it will be an offence to be found in possession of such an item without being able to give a satisfactory exculpatory account of such possession,*

(vi) **Unlawful tools**: unlawfully and intentionally use, possess, manufacture, assemble, obtain, sell, purchase, make available or advertise any software or hardware tool to commit the above cybercrimes;

(vii) **Cyber fraud**: unlawfully and with the intention to defraud make a misrepresentation by means of data or a computer program or through any interference with a system which causes actual prejudice or is potentially prejudicial;

(viii) **Cyber forgery and uttering:** unlawfully and with the intention to defraud make or pass off false data or a false computer program to the actual or potential prejudice of another person is guilty of the offence of cyber forgery or uttering; or

(ix) **Cyber extortion:** It will be an offence to unlawfully and intentionally threaten to commit or commit certain cybercrimes to obtain any advantage from another person or compelling another person to perform or to abstain from performing any act.

Note *that it will be an offence to attempt, conspire, aid, abet, induce, incite, instigate, instruct, command or procure a cybercrime, and that a cybercrime would apply in addition to other offences (such as the common law offence of theft) and other cybecrimes (see eg section 15 competent verdicts).*

In addition, a cybercrime can become an aggravated offence if:

(i) A restricted computer system (under the control of, or exclusively used by, any financial institution, organ of state or critical information infrastructure) is involved;

(ii) It endangers a life;

(iii) It violates physical integrity or physical freedom or causes bodily injury;

(iv) It causes serious risk to the health or safety of any segment of the public;

(v) It causes the destruction of or substantial damage to any property;

(vi) It causes a serious interference with, or serious disruption of an essential service, facility or system, or the delivery of any essential service;

(vii) It causes any major economic loss;

(viii) It creates a serious public emergency situation; or

(ix) It prejudices the security, the defence, law enforcement or international relations of the Republic.

Malicious communications

The Draft Bill will also make provision for offences relating to malicious communications:

(i) **Incitement offence**: It will be an offence to unlawfully make available, broadcast or distribute a data message via a computer system with the intention to incite violence or property damage.

(ii) **Harmful messages**: It will be an offence to unlawfully and intentionally make available, broadcast or distribute a data message via a computer system which is harmful (threatens violence or property damage; intimidates, encourages or harass a person to harm himself or herself or any other person; or is inherently false in nature and it is aimed at causing mental, psychological, physical or economic harm).

Note *that the offence will require that a reasonable person in possession of the same information and with regard to all the circumstances would regard the data message as harmful.*

(iii) **Intimate distribution**: It will be an offence to unlawfully and intentionally make available, broadcast or distribute a data message via a computer system of an intimate image (as defined) of an identifiable person knowing that the person depicted in the image did not give his or her consent thereto.

(iv) **Protection order**: Provision will be made for an order to protect a complainant pending finalisation of criminal proceedings to prohibit further distribution and to require an electronic communications service provider or person in control of a computer system to remove or disable access to the data message in question and/or to provide prescribed particulars to the court (within 5 ordinary days).

Note that in certain instances *the* court may also order a Protection from Harassment Act protection order.

Offences for financial institutions, electronic communications providers and others

The Draft Bill proposes mandatory "deputy" requirements:

(i) **Duty to assist**: It will be an offence for an electronic communications service provider, financial institution or person, other than the person who is suspected of having committed the offence which is being investigated, who is in control of any container, premises, vehicle, facility, ship, aircraft, data, computer program, computer data storage medium or computer system that is subject to a section 27(1) search not to, if required, provide technical assistance and such other assistance as may be necessary, to a police official or investigator in order to search for, access and seize an article.

(ii) **Preservation and data orders**: It will be an offence for an electronic communications service provider, financial institution or person to fail to comply with an expedited preservation of data direction or with a preservation of evidence order or with a data direction order, or disclose any data to a police official on the strength of an expedited preservation of data direction (unless it is authorised);

(iii) **Assist foreign authorities orders**: It will be an offence for a person, electronic communications service provider or financial institution not to comply with an order to assist a foreign authority or to provide false information in relation to the order;

(iv) **Reporting duty**: It will be an offence for an electronic communications service provider or financial institution that is aware or becomes aware that its computer system is involved in the commission of any category or class of cybercrimes (as decided and gazetted by the Minister of Police from time to time) to fail to:

- without undue delay and, where feasible, report the offence to SAPS as prescribed within 72 hours after having become aware; or
- preserve any information which may be of assistance to the law enforcement agencies in investigating the offence; and

Note *that subject to any other law or obligation (?), this offence must not be interpreted as imposing duties on an electronic service provider or financial institution to monitor the data that it transmits or stores or to actively seek facts or circumstances indicating any unlawful activity.*

Also note *that this offence does not apply to a financial sector regulator or a function performed by the South African Reserve Bank in terms of section 10 of the South African Reserve Bank Act.*

(v) **Critical infrastructure duty**: If declared a critical information infrastructure then it will be offence to fail, without reasonable cause, to timeously take satisfactory steps to comply with a directive compliance notice.

Related matters

The following ancillary matters are proposed in the Draft Bill:

(i) **Jurisdiction**: The Draft Bill proposes wide jurisdiction grounds, including extra-territorial application;

(ii) **Search and seizure**: The Draft Bill proposes, amongst others, search and seizure without a warrant if the person who has the lawful authority to consent thereto consents in writing to such search, access or seizure;

Note that this provision is made subject to any other law, and also see section 43 search for access to data and seizure of data where no authorisation is required.

(iii) **Arrest**: Arrest provisions include that a police official may, amongst others, without a warrant, as contemplated in section 40 of the Criminal Procedure Act, arrest any person whom he or she reasonably suspects of having committed a cybercrime or malicious communication offence (and then perform certain search and seize powers);

(iv) **Police official and investigator behaviour**: The Draft Bill proposes measures to protect legitimate rights and confidential information, and address repugnant behaviour by officials such as giving false information;

Note *that similar concerns may exist regarding the evidence by affidavit suggestions.*

(v) **Mutual assistance**: The Draft Bill proposes sharing information with foreign states - also see agreements with foreign states;

(vi) **24/7 point of contact**: The Draft Bill proposes establishing another regulatory entity to ensure immediate expedited assistance for the purpose of proceedings or investigations regarding the commission or intended commission of a cybercrime, malicious communications offence, any other offence in terms of the laws of the Republic which may be committed or facilitated by means of an article, or similar offences committed by or facilitated through an article in a foreign State;

(vii) **Cyber security structures**: The chapter regarding the security clusterfunction includes the proposal that, subject to any other law, the Minister responsible for the administration of justice must make regulations to regulate information sharing, for purposes of this Chapter, regarding cybersecurity incidents and the detection, prevention, investigation or mitigation of cybercrime;

(viii) **Critical information infrastructure**: The State Security Agency will determine who falls under this category and affected financial institutions, non-governmental entities etc will be given some opportunity to make representations and thereafter listed infrastructure must comply with the Minister responsible for State Security's directives on:

- the classification of data held by the critical information infrastructure;
- the protection of, the storing of, and archiving of data held by the critical information infrastructure;
- cybersecurity incident management by the critical information infrastructure;
- disaster contingency and recovery measures which must be put in place by the critical information infrastructure;
- minimum physical and technical security measures that must be implemented in order to protect the critical information infrastructure;
- the period within which the owner of, or person in control of a critical information infrastructure must comply with the directives; and

- **any other relevant matter** which is necessary or expedient in order to promote cybersecurity in respect of the critical information infrastructure.

www.justice.gov.za

Back to index

Information

03. Protected Disclosures Act: Amendment Bill

The proposals contained in the Amendment Bill 2015 version B raise both welcome compliance measures and unnecessary regulatory risks. It is respectfully suggested that the Act is of fundamental importance and that the Draft Bill should have been given a longer comment period, and more prominence than on a department website.

Always potentially relevant law

Current: Any non-compliance by an employer in terms of any law that relates to its business may trigger the Protected Disclosures Act - see definition of disclosure.

Bill proposal: Add the Employment Equity Act unfair discrimination sections in the definition of disclosures, which will include the uncertainty created by the future "discrimination on arbitrary grounds".

***Note**: The Employment Equity Act unfair discrimination sections would be included in the definition of disclosures in any event under failure to comply with any legal obligation to which that person is subject.*

Past employees included

Current: The Act currently aims to protect employees that make protected disclosures in terms of the Act - see definition of employee. The Act is also intimately linked to other laws, and amendments to it will have a knock-on effect to several of them:

(i) If the employer is a company then the Companies Act whistleblowing section must also be considered (non-employee trade union, employee representative, supplier, supplier employee and shareholder whistleblowing must currently be considered under that section and not this Act);

(ii) Environmental risk whistleblowing is also protected under the National Environmental Management Act (which triggers consideration of the extensive list of environmental laws - see related laws on left side of NEMA);

(iii) Employers and employees should also note the Labour Relations Act definition of unfair labour relations practice, automatically unfair labour practices, proposed inquiry by arbitrator and disputes about unfair dismissals sections;

(iv) Employers and employees must understand that where this Act gives a discretion to make a non-compliance disclosure, there are many legal provisions that make it an **offence not to make a disclosure** (for example the duty to report if a child is abused, neglected or in need of care and protection);

(v) Pension funds and pension fund trustees need to note the revised application of the Protected Disclosures Act to pension funds (see Pension Funds Act disclosure and protected disclosure definitions and protection of disclosures); and

(vi) Municipalities and municipal entities should note the application of the Protected Disclosures Act in terms of the general provisions of the financial misconduct procedures and criminal proceedings regulations.

Bill proposal: Include protected disclosures by past employees, and define business as including the whole or part of any business, trade, undertaking or service (see definition of employees).

***Note**: The proposed definition gives no parameters or cut-off date so that anyone who worked for any period in the past for an employer, theoretically has a right to make a protected disclosure.*

Workers included

Current: As mentioned, the Act is about protecting employees against occupational detriments suffered due to a protected disclosure made about their employer - an employee may wish to take the best legal advice they can (during a protected disclosure to a legal advisor), or the advice of the public protector (during a protected disclosure to the public protector) regarding protecting their physical safety if there is a genuine concern that their lives may be in danger if they disclose.

Bill proposal: The Bill wants to extend protected disclosures to any person who works or worked (see **past employees** note above) for another person or for the State, or in any manner assists or assisted in carrying on or conducting or conducted the business of an employer or client, as an independent contractor, consultant, agent

or person rendering services to a client while being employed by a temporary employment service (see definition of worker).

***Note**: Service providers are drawn into the net which may increase regulatory uncertainty. The definition also creates an interesting interplay with the Companies Act whistleblowing section - depending where statutory interpretation ends up these persons could be depicted as suppliers, and if suppliers of a company would in future, like employees, have to comply with both Acts requirements, which would be positive except for the occupational detriment proposal below.*

Duty to take action

Current: The Act allows that protected disclosures may be made to employers.

Bill proposal regarding employer disclosure: Every employer must authorise appropriate internal procedures for receiving and dealing with information about improprieties, and take reasonable steps to bring the internal procedures to the attention of every employee and worker.

Bill proposal regarding feedback: An employer that received a protected disclosure must:

> (i) Within 21 days after receiving it acknowledge receipt in writing and notify the employee or worker of the investigation steps to be taken and, where possible, the timeframe within which the investigation will be completed; and
>
> (ii) Investigate or, where necessary, refer the disclosure to another person or body if it could be more appropriately investigated or dealt with by that other person or body (who have their own similar notification duties).

Exceptions will be allowed where the employer does not know the identity and contact details of the employee or worker who has made the disclosure, or where it is necessary to avoid prejudice to the prevention, detection or investigation of a criminal offence.

Similar duties are proposed for the Public Protector, the Auditor-General, a member of Cabinet or a member of the Executive Council of a province when they receive a protected disclosure.

***Note**: It makes good sense that employers continuously ensure an effective protected disclosure system is in place, that disclosures are addressed appropriately and that employees perceive the system as being objective and secure. There does not seem to be a sanction for failure to investigate and keep the protected discloser informed in the Act, but a number of other laws, such as accessory to a corruption offence or after a corruption offence, may be triggered.*

Employer client liable for employer actions

Current: The Act currently applies to protected disclosures about employers.

Bill proposal: Where an employer, under the express or implied authority or with the knowledge of a client, subjects an employee or a worker to an occupational detriment, both the employer and the client will be jointly and severally liable.

***Note**: This phrase should be revisited and reworded, in terms of Constitutional balancing and other general legal principles to create more clear and more balanced parameters, as its current text seems to create limitless and unjustified liability for any client for simply being aware of an occupational detriment caused by another over which they may have no control over.*

Remedies

Current: The Act provides for remedies against occupational detriment.

Bill proposal: Amongst others, specific reference in the remedies provision is made to allow anyone to approach a court for appropriate relief including payment of compensation by the employer to that employee or worker, payment by the employer of actual damages suffered by the employee or worker, or an order directing the employer to take steps to remedy the occupational detriment.

***Note**: This is in order where a court is involved, as they are still predominantly guided by the Constitution and legal principles such as 'hear the other party'. It is not certain how tribunals (available route for employees) will apply general legal principles.*

Exclusion of liability

Bill proposal: A court may find that an employee or worker who makes a protected disclosure of information that tends to show that a criminal offence was, is being or is reasonably likely to be committed shall not be liable to any civil, criminal or disciplinary proceedings by reason thereof, if such disclosure is prohibited by any other law, oath, contract, practice or agreement requiring him or her to maintain confidentiality or otherwise restricting the disclosure of the information with respect to a matter. Exclusion of liability does not extend to the civil or criminal liability of the employee or worker for his or her participation in the disclosed impropriety.

***Note**: The common law right to legal privilege is fundamental to our law, and the High Court has an inherent right to set aside this privilege where it is clearly being abused. Such an important discretion should not be left to a magistrate court or other forum. In addition, the lack of Constitutionally balanced and reasonable parameters (such as not differentiating offences when some regulators choose to make almost anything an offence) may change this positive law into a **high regulatory risk for businesses**. Finally, this proposed section cannot by default override the Constitution, and its Constitutional laws (such as the Protection of Personal Information Act, Promotion of Access to Information Act, Promotion of Administrative Justice Act etc).*

Liability for fraudulent disclosure

Bill proposal: An employee or worker who intentionally discloses false information, knowing that information to be false or not knowing or not believing it to be true, is guilty of an offence and is liable on conviction to a fine and/or to imprisonment for a period not exceeding two years, **if** the Director of Public Prosecutions decides to take action.

***Note**: This is a theoretically positive provision but enforcement may be missing, fine may be far less than damage caused to employer, its shareholders, its clients etc, and liability should be extended to a person appearing on behalf of discloser etc. Other laws regarding criminal fraud etc may apply in such situations and should be considered. This liability should also be considered for the other whistleblowing laws mentioned under the heading **past employees included**.*

Safety

04. Medicines and Related Substances Act: Draft Regulations

The draft amendments to the General Regulations (comment deadline 3 months from 27 January 2017) propose, amongst others:

(i) Overhauling licensing, registration, prescription details, import, export, registers, and vigilance requirements;

(ii) Key definition changes, including complementary medicine, health supplements, sweetener;

(iii) Increased conditions for compounding medicines, including prohibition on advertising or export;

(iv) That an applicant for registration of medicine, medical device or IVD will be informed as soon as practically possible;

(v) That the Authority may add conditions before accepting an application to import a medicine;

(vi) Increased labelling conditions, including tracking barcode/GMO warning in complementary medicines;

(vii) Increased professional information requirements, including the name of a sugar used or 'sugar free' or 'contains sweetener' and further information that the Authority may request above that stated in the regulation;

(viii) Increased consumer leaflet requirements, including warnings on central nervous system function modifying properties, and how to obtain the professional information related to the medicine;

(ix) Increased permanent record conditions, including ID number and unique dispensing identifier;

(x) Further limitation on personal medicinal use by persons entering South Africa;

(xi) Wholesalers desiring to buy medicines from another wholesaler may apply for exemption;

(xii) Medicines and scheduled substance may only be destroyed at an authorised waste disposal facility, and must be destroyed in such a manner that it cannot be salvaged again;

(xiii) Repackaged medicine must have a batch numbering system linking it to original packaging; and

(xiv) Increased veterinary medicine labelling conditions, including warning on withdrawal period where relevant.

GN858 GG40158 / 25 July 2016 (Incorporated into the Medicines and Related Substances Act and Regulations)

Safety

05. Occupational Health and Safety Act: Draft Ergonomics Regulations

The Draft Ergonomics Regulations (comment deadline 90 days from 27 January 2017) propose, amongst others:

(i) Defining ergonomic risk factors as actions in the workplace and/or workplace conditions which may cause or aggravate a work-related-musculoskeletal-disorder;

(ii) Targeting employers and self-employed persons (where physical or cognitive ergonomic risk factors may be present), as well as designers, manufacturers, erecters, installers or suppliers of machinery, equipment or articles for use at work

(iii) Requiring that employers pay an ergonomics competent person to train employees before placement and at regular intervals, that employers give adequate information, instruction and training with regards to ergonomics, and that employers keep a training record;

***Note**: It would be preferable that there be a possibility of applying for an exemption in cases where ergonomics risk factors may exist but are practically low in likelihood and do not reasonably warrant the full or part costs associated with a trainer etc.*

(iv) Reiterating the duty of persons exposed to ergonomic risk factors to obey lawful ergonomic instructions;

(v) Requiring that affected designers eliminate ergonomics risk factors (or mitigate if elimination is not reasonably possible), and provide prescribed information to manufacturers and users;

***Note**: Designers, manufacturers and suppliers should also consider the interaction of this law with the Consumer Protection Act duties, where applicable, for example fair value, good quality and safety requirements.*

(vi) Requiring that affected manufacturers and suppliers make an item as safe as reasonably possible (including in relation to its construction, transport or installation), and give prescribed information for potential users on how to use and maintain items;

***Note**: Manufacturers must also use and test relevant designer safety measures.*

(vii) Requiring that employer must conduct a prescribed risk assessment, record the results, review the assessment. and ensure that employees under control of the employer are informed, instructed and/or trained accordingly by a competent person, before they start work or when a review takes place;

(viii) Requiring that employers and self-employed persons must prevent exposure to ergonomics risk factors (or adequately control such ergonomics risk factors where this is not reasonably practicable);

(ix) Introducing ergonomics specific medical surveillance, control maintenance, records, appeals and offences.

***Note**: Ergonomics consideration represent a sub-consideration of the general duty to, as far as reasonably possible, consider the safety of employees and safety of persons on the premises (and manufacturer/supplier duty where relevant). In other words, the draft ergonomics regulations suggest more specific means to manage the general duty, and every proposed requirement should preferably echo the key phrase of the Act "as far as reasonably possible".*

GNR64 GG40578 / 27 January 2017 (Incorporated into the Occupational Health and Safety Act and Regulations)

Back to index

General

06. Notable One Liners

Draft Ballast Water Management Bill 2017: Extended opportunity has been given to comment (30 days from 10 February 2017) on the Draft Bill, which will be incorporated into the website in due course.

Compensation for Occupational Injuries and Diseases Act: A new return of earnings form is available from 10 February 2017 from the Department of Labour.

Competition Act: The Western Cape citrus producers forum exemption approval has been extended to 16 March 2017.

Criminal Procedure Act: The Criminal Procedure Amendment Bill 2017 proposes addressing the constitutionally invalid compulsory imprisonment or hospitalisation requirements contained in the capacity to understand chapter.

Criminal Law (S Offences and Related Matters) Amendment Act: The Draft Cybercrimes Bill proposes a 'harmful disclosure of certain material' offence which may trigger removal and disabling duties for electronic communications providers, and offences relating to certain material depicting a child (including failure to report knowledge or a reasonable suspicion of such an offence asap to the SA Police Service and live performance and recruitment offences), and increased sentences for certain offences.

Criminal Procedure Act: The Draft Cybercrimes and Cybersecurity Bill proposes repealing the Correctional Services Act offence of unauthorised access to or modification of computer material, stricter bail considerations for certain cybercrimes, minimum sentencing for certain cybercrimes, and adding certain cybercrimes to the Child Justice Act mid-/most serious categories.

Customs and Excise Act: A new rule has been gazetted for the environmental levy imposed on certain tyres manufactured in South Africa or imported into South Africa.

Disaster Management Act: The Draft Cybercrimes and Cybersecurity Bill proposes including damage or disruption to critical information infrastructure in the definition of disaster.

Electronic Communications and Transactions Act:

(i) The Draft Cybercrimes and Cybersecurity Bill proposes repealing provisions relating to protection of critical databases, cybercrimes and jurisdiction.

(ii) Notice has been gazetted for licensees to complete a questionnaire, for purposes of assisting with the review of the pro-competitive conditions in the call termination regulations.

Films and Publications Act: The Draft Cybercrimes and Cybersecurity Bill proposes repealing the section relating to prohibition, offences and penalties on possession of films, games and publications, despite Amendment Bill 2015 proposals to substitute that section.

Financial Intelligence Centre Act : The Draft Cybercrimes and Cybersecurity Bill proposes repealing the provisions relating to unauthorised access to computer system or application or data and unauthorised modification of contents of computer system, and their related definitions.

Legal Practice Act: A Code of Conduct as been gazetted, that will apply when the relevant parts of the Legal Practice Act have commenced, and that will be incorporated and overviewed on www.gazette.co.za in due course.

Local Government Municipal Finance Management Act : Municipalities and municipal entities have been exempted, subject to conditions, from the requirement that new and existing financial and supply chain management officials must meet minimum competency levels.

Medicines and Related Substances Act: The method of calculating the dispensing fee was amended 27 January 2017.

National Environmental Management Act: The Mapungubwe cultural landscape world heritage site environmental management framework has been gazetted.

National Environmental Management Biodiversity Act:

(i) Draft norms and standards for the management and monitoring of hunting of leopard in South Africa for trophy hunting purposes have been gazetted (Comment deadline 30 days from 8 February 2017).

(ii) The draft prohibition on rhino horn derivatives (comment deadline 30 days from 8 February 2017) proposes prohibiting the powdering of rhino horn; rhino horn slivers, chips, drill bits and similar derivatives; and the removal of parts or layers of a rhinoceros horn. The prohibition would not apply where a person inserts a microchip into a rhino horn; dehorns or takes a part off a rhino horn for management intervention or security purposes; takes a sample taken for genetic profiling (as per the relevant norms and standards. It would also not apply where powder, sliver, chip, drill bit or derivatives were formed/ or a layer removed by a registered scientific institution for scientific purposes (or for genetic profiling as per norms and standards).

(iii) The draft regulations for domestic trade in rhino horn, products and derivatives (comment deadline 30 days from 8 February 2017) propose regulating the domestic selling or otherwise trading in, giving, donating, buying, receiving, accepting, disposing or acquiring rhino horn in SA, and the export of rhinoceros horn for personal purposes from SA.

(iv) A draft listing of the Eastern Black Rhinoceros as a protected species has been gazetted (Comment deadline 30 days from 8 February 2017).

National Environmental Management Protected Areas Act: The draft cultural heritage survey guidelines and assessment tools for protected areas in South Africa has been gazetted (Comment deadline 30 days from 3 February 2017). ***Note****: This useful tool also serves as a general reminder that the ambit of our environmental laws include the cultural environment*.

National Prosecuting Authority Act: The Draft Cybercrimes and Cybersecurities Bill proposes repealing provisions relating to unauthorised access to or modification of computer material.

National Regulator for Compulsory Specifications Act: Reminder that the compulsory specification for live lobster harvesting, preparation, packing, conveyance, quality and hygiene will commence 19 February 2017.

National Water Act: A Richards Bay emergency government waterworks declaration has been gazetted, which means that limited environmental impact assessment processes will apply.

Pension Funds Act : Clarification has been gazetted that the default regulations are in fact draft regulations, and a comment deadline (28 February 2017) has been provided. You may also wish to consider the updated past overview.

Protection of Constitutional Democracy against Terrorist and Related Activities Act: The Draft Cybercrimes and Cybersecurity Bill proposes making destruction or substantial damage or interference with a critical information infrastructure or any part thereof a terrorist activity, and making certain supplies of software or hardware tools an offence connected with terrorist activities.

Public Finance Management Act: The Industrial Development Corporation of South Africa Limited has been exempted until 26 January 2020 from the requirement to promptly inform National Treasury on any new entity it intends to establish or in the establishment of which it takes the initiative (and to allow the National Treasury a reasonable time to submit its decision prior to formal establishment), and from the requirement for accounting authorities to submit certain information. It seems the exemption is limited to a domestic transaction below a rand value of R250 million.

Regulation of Interception of Communications and Provision of Communication-related Information Act: The Draft Cybercrimes and Cybersecurity Bill proposes adding cybercrimes as offences that may warrant an interception or real-time or archived communication-related directions.

Road Accident Fund Act:

(i) The Road Accident Fund Amendment Bill 3 of 2017 proposes, amongst others, a single medical tariff, further regulating liability of the Fund and legal proceedings against the Fund, prescribing tariffs

and what constitutes serious injuries, allowing for cost contributions, further limit funeral costs, and extending the application of prescription of claims).

(ii) As from 31 January 2017, where a claim for compensation includes a claim for loss of income or support, the annual loss of income or support, irrespective of the actual loss, must be proportionately calculated to an amount not exceeding R254 450 per year in the case of a claim for loss of income, and R254 450 per year in respect of each deceased breadwinner, in the case of a claim for loss of support.

Skills Development Act: The appointment of the Safety and Security SETA administrator has been extended to 12 August 2017.

South African Police Services Act: The Draft Cybercrimes and Cybersecurity Bill proposes repealing the offence related to unauthorised access to or modification of computer material.

Special Investigating Units and Special Tribunals Act:

(i) An investigation has been launched into a number of actions that may involve the Harry Gwala District Municipality councillors, officials and employees and K and M Security Service CC, Emangomeni Trading Enterprise CC, Tricircle Hardware, Kaltravel CC, Garden Court Hotel, Protea Hotel, Busiya Consulting CC, Mini Construction and Msomi Test Pump and Installation and Borehole Repairs and Cyclone Construction.

(ii) An investigation has been launched into matters relating to the KZN Department of Agriculture and Rural Development and Mjindi Farming (Pty) Ltd.

(iii) An investigation has been launched into the affairs of the Mopani District Municipality.

Traditional Courts Bill: The Bill proposes, amongst others, prohibited conduct that must be regularly reviewed (with some examples given) and that a traditional court may only hear and determine a traditional court matter (including key family and property issues such as advice relating to customary law practices in respect of custody and guardianship of minor or dependent children, and succession and inheritance) if the party against whom the proceedings are instituted agrees freely and voluntarily to the resolution of the dispute by the traditional court in question. ***Note****: The Draft version of the Bill was not made available for public comments, with the stated intent being that Parliament may later request public submissions*.

Back to index

SAIPA member log-in details and support

Please DO NOT register on www.gazette.co.za if you are a SAIPA member (unless you wish to add a non-SAIPA member) as SAIPA has given members full access to the website.

To access www.gazette.co.za and www.rmonline.co.za simply use the following:

- Username: first initial + surname + last two digits of membership number (e.g. pstassen32)
- Password: full membership number (e.g. 5432).

Contact support@gazette.co.za for log-in queries or if you wish to change your personal details. Please note that if you are **not** receiving the newsletter twice a month you may need to ask your IT department to check whether it is being blocked by your IT systems or check that SAIPA has your newest email address.

Kind regards,

SAIPA Technical and Standards Department

Back to index