SABPP FACT SHEET

NUMBER 2014/2: March 2014

PROTECTION OF PERSONAL INFORMATION ACT

1. Introduction

The Protection of Personal Information Act, No 4 of 2013, has been signed into law by the President and gazetted on 26 November 2013, but the Act will only commence on a date yet to be proclaimed by the President. Once the commencement date is proclaimed, "responsible parties" (for our purposes, that is the employer) will have a one-year transition period to ensure that the processing of personal information, whether internally or through service providers, is compliant with the Act.The one-year period may be extended by the Justice Minister in respect of different class or classes of information bodies by an additional period which may not exceed 3 years. Therefore the commencement may be staggered over a period of time. The current view is that the commencement date may be proclaimed in approximately 6 months , therefore one is looking at an 18 month grace period.

The Act is considered by experts to be well drafted and brings South Africa up to, if not exceeding, the best international best practice for protecting people's personal information and preventing identity theft. The Act is based on the European Union legislation and incorporates some lessons learned from the EU. In our modern times, where computer and telephonic devices process huge amounts of data, much of which is personal, solid forms of legal protection are required The Act gives effect to an individual's constitutional right to privacy by safeguarding personal information when processed by public or private bodies, subject to justifiable limitations. The Act therefore balances the right to privacy and the right of access to information. The Act's focus is not privacy, as such, but rather data protection in the information age. It aims to regulate the manner in which data is processed and every aspect of the processing of personal information from its collection to its destruction.The Act will have significant consequences for all businesses that process the personal information of individuals or juristic persons. It will impact on all companies and businesses that process information relating to employees,

customers, suppliers and other third parties, such as financial services and marketing organisations. There is no doubt the Act will impact quite heavily on the Human Resources function and add to its compliance responsibilities.

It is therefore important that HR practitioners develop an understanding of the 8 conditions for the lawful processing of personal information and are able to apply those principles to the processsing of employees' personal information in their organisations. As the eight conditions for the lawful processing of personal information will affect nearly every area of business that processes personal information, the consequences are that this will require behavioral changes, changes to legal documents, internal structural changes (i.e. information technology upgrades, assurances that a data base cannot be accessed and physical firewalls and safety measures), analyses of subcontracting practices and gaining control over cross-border data flows

"The Act will apply to any information regarding clients or suppliers, including contact details and correspondence. Human resources and payroll data, curricula vitae, applications for employment, CCTV records, performance reviews and internal e-mail records are also subject to its requirements, which could have a significant impact on the way local entities conduct business."

Heino Gevers, Security Specialist at Mimecast South Africa, quoted on ITWeb

This Fact Sheet will cover key aspects of the Act and will highlight important implementation issues for HR practitioners.

2. What is "personal information"?

The Act defines "personal information" as information which relates to an identifiable, living, natural person or identifiable juristic person including, but not limited to:

a) Information relating to the following :
   - Race, national/ethnic/social origin/colour
   - Gender/Sex
   - Pregnancy
   - Marital status
   - Sexual orientation
   - Age
   - Physical or mental health/well-being/disability
   - Religion/conscience/belief
   - Culture/language
   - Birth.

b) Information relating to the education, medical, criminal, financial or employment history of a person.

c) Any identifying number, symbol, e-mail address, telephone and physical address, location information, online identifier or other particular assignment to the person.

d) Biometric information.

e) Personal opinions, views or preferences of the person.

f) Explicitly or implicitly private or confidential correspondence.

g) Views of others about that person.

h) Name if it appears together with other personal information about that person of if the name would reveal information about that person.

This definition basically means that all information about an employee must be treated as personal information except maybe working time information used to calculate pay. Salary and benefit information would be included as personal information, however where this information is provided and is not identifiable to any particular person it may fall within the exceptions/exemptions in the Act.

3. Special personal information

Some of the above categories and some additional ones fall under the scope of what is termed "special personal information". The processing of special personal information is prohibited unless there is consent, or it is required for the establishment, exercise or defence of a right or obligation in law etc. This includes information on religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health and sexual life, biometric data or criminal behaviour as specified.

In practice, the gender and race of an employee is relevant for the purposes of the Employment Equity Act. Regarding trade union membership, whilst the exemption applies to the union, in order to have a stop order processed for union membership the employee would need to complete a stop order and provide the necessary consent.

4. Data Protection Conditions

The Act lays down eight conditions which must (all) be satisfied in order for any processing of personal information (manual or automatic and including storage, dissemination by any means, and destruction) to be lawful. Because storage and destruction are included in this definition of processing, historical information about employees is also subject to the Act. Basically, if the information is collected with the knowledge and consent of the data subject, and is clearly linked to an explicit and reasonable purpose and it is carefully looked after and only used for that purpose and is not kept for longer than is necessary, the processing of that data will comply with the requirements of the Act..

1. **Accountability.** A responsible party (the employer) must ensure all conditions are complied with and that the information is obtained fairly and lawfully. Therefore an Information Officer must be appointed, whose duty it is to ensure compliance with the provisions of the Act because even if an operator is engaged or it is outsourced, the responsible party is still liable.
2. **Processing Limitation.** Personal information may only be processed if the following are satisfied (all of them as applicable):
    a. It is processed lawfully and in a reasonable manner;
    b. It is adequate, relevant and not excessive given the purpose for the processing;
    c. The data subject (in this case, the employee (and his/her dependants for benefit schemes)), consents;
    d. The processing is necessary for the performance of a contract (in this case therefore, for processing aspects of the contract such as pay, performance, benefits etc);
    e. The processing is required by any law (this would cover aspects of health and safety and probably also aspects covered by the Basic Conditions of Employment Act, the Employment Equity Act and the Skills Development Act);

f. The processing "protects a legitimate interest" of the employee (this would probably cover recording skills for the purposes of skills training or development);

g. The processing is carried out by a public body for the proper performance of its public law duty (in this case, for example, CCMA, SAQA and Department of Labour officials)

h. The processing is "necessary for pursuing the legitimate interests of the responsible party (the employer) or of a third party to whom the information is supplied (in this case for example an employee benefit provider or in recruitment where the collection becomes relevant).

A data subject (employee) may object on reasonable grounds to the processing of his/her personal information, and the responsible party may not then process that information.

All personal information must be collected directly from the data subject unless the data subject consents that it can be collected from a third party for the following reasons:

- It is in the public record/deliberately been made public by the employee e.g. twitter, face book etc.
- It will not prejudice the data subject;
- It is necessary e.g. to enforce a law
- If direct collection would prejudice lawful purpose of collection
- Not reasonably practicable to collect directly given the circumstances.

3. **Purpose specification.** Personal information must be collected for a specific, explicitly defined and lawful purpose related to a function or activity of the responsible party (employer) and the data subject must be aware of this purpose. Retention of records must not be for longer than that required for the purpose for which it was collected. This has vast and far-reaching implications from an HR perspective. Generally there are additional employment laws specifying how long certain information must be retained for.

4. **Further processing limitation.** Personal information may not be processed further (presumably this means, for example, moving it to a different database) unless such further processing is compatible with the purpose for which it was first collected. There are specific guidelines on whether further processing is compatible and certain exemptions.

5. **Information Quality.** The responsible party (employer) must take reasonable steps to ensure that the information is complete, accurate, not misleading and is updated where necessary. (This condition equates to good practice for data management which should be in place anyway.) For example, employees should be allowed to know what personal information is on record and given the opportunity to update such information possibly on an annual basis.

6. **Openness**. The responsible party must take reasonable steps to ensure that the data subject is aware of what information is collected, from what source, who is responsible and what the purpose of collecting the information is, whether it is voluntary or mandatory, the consequences of failing to provide the information, any law authorising or requiring the collection of information, whether the information will be transferred to a third country or international organisation and the level of protection afforded to the information transferred. Data subjects must be made aware of their right to access and rectify information or object to the processing of the information and the right to

lodge a complaint to the Regulator. It is paramount that an employer keeps records of what it processes.

7. **Security Safeguards**. The responsible party must take reasonable steps to prevent the loss of, damage to, unauthorised destruction, unlawful access to or unlawful processing of personal information. Internal and external risks must be assessed, safeguards must be implemented and updated, and generally accepted security practices and procedures should be adhered to. If there is a breach, the data subject and the Regulator must be informed as soon as possible.

8. **Data Subject Participation**. The data subject has the right to request confirmation from the responsible party as to whether it, or another third party, is holding personal information and what information is held. The data subject has rights, subject to certain limitations, to request that inaccurate/irrelevant/out-of-date/excessive/incomplete/unlawfully obtained information be corrected or deleted. Clearly therefore, the employer must put in place procedures catering for this.

Clearly, several of the above conditions are designed to limit processing of information such as telephone numbers and email addresses by unwanted marketing agencies rather than to limit processing of employment related information, but the conditions must be carefully scrutinised for implications in relation to employee information.

There is a provision that information may not be sent to a foreign country unless the responsible party ensures proper protection of that information, either by relying on the laws of the country or by contract between the sending and receiving parties.

The Act allows the collection and processing of personal information for statistical and research purposes with less onerous conditions.

5. Enforcement of the Act

Enforcement is the responsibility of an Information Regulator, an independent office reporting to the National Assembly. This will be set up as part of the implementation of the Act.

Aggrieved data subjects may lay complaints with the Regulator (to be appointed by the Minister of Justice) whose office must investigate complaints and attempt to resolve the dispute through conciliation and mediation.

The Regulator will also have powers to make an assessment of any responsible party for compliance with the Act, either in response to a complaint or independently. The Regulator may issue an enforcement notice to the responsible party, who may request the Regulator to cancel or amend the enforcement notice. Warrants may be obtained from a judge of the High Court or a regional magistrate to enter and search premises if it appears there is a contravention of the legislation.

Appeals may be made to the High Court, either by a complainant not satisfied by the result of the Regulator's dispute resolution or by a responsible party against an enforcement notice.

Claims for civil damages may also be pursued through the courts by aggrieved data subjects. The important issue here is that civil remedies for damages for any breach in terms of section 73 are regardless of whether or not there was intent or negligence on the part of the responsible party. Some HR implications

6. Appointment of Information Officer

The Chief Executive Officer or equivalent of each responsible party is designated as the Information Officer and may authorise another person to carry out the duties. The name of the designated person must be registered with the Regulator. These duties are:

- To educate, encourage and ensure compliance
- To deal with requests as described in the Act
- To work with the Regulator on investigations instigated under the Act.

Deputy Information Officers may also be appointed. We recommend that a formal appointment be made of a Deputy Information Officer for matters relating to employee personal information.

7. Obtaining consent of employees to the processing of personal information

Section 18 of the Act lays down the steps that must be taken to ensure that a data subject is aware of the nature of the information being collected, why it is being collected, who will have access to it, whether the collection is mandatory or voluntary and what right the data subject has to object or lay a complaint.

It should be noted that an employee would find it difficult to object regarding any personal information that he/she has already posted onto social media.

It is recommended therefore that legal advice be sought on a suitable clause to be inserted into any form that is completed by applicants or employees (remember that applicants will also be data subjects), and a suitable clause for contracts of employment. It will probably be necessary for a document to be drawn up for signature by all present employees, giving consent to the processing of their personal information. Any change contemplated to contracts of employment must go through a consultation process with affected employees and/or their representatives.

8. Confidentiality

HR practitioners will fall under the category of persons who, under the Act, process information on behalf of a responsible party. The Act requires such persons to:

- process such information only with the knowledge or authorisation of the responsible party; and
- treat personal information which comes to their knowledge as confidential and must not disclose it,

unless required by law or in the course of the proper performance of their duties.

Proper documentation of HR business processes and systems will supply evidence supporting the first requirement.

Keeping employee information confidential is a primary duty of all HR practitioners and they should not need to be reminded of this by the law. The SABPP's Code of Conduct emphasises this point, and it is once

again emphasised in the SABPP HR Competency Model. The wide definition of "personal information" in the Act is a salutary reminder to HR practitioners that verbal discussions, opinions and similar information must also be regarded as confidential.

It is vitally important that contracts, policies and procedures are audited and where necessary amended.

9. Due diligence in mergers and acquisitions

Due diligence exercises often involve collection of employee demographics, pay and benefits data and other risk-related information. Provided that employee names or other means of identification are de-linked from any information provided, a due diligence exercise would not contravene the Act.

10. International payrolls or employee databases

An evaluation must be conducted for each country receiving personal information on South African employees (employees falling under South African legal jurisdiction) as to whether acceptable information protection laws exist. If not, a suitable contract must be drawn up between the South African employer and the party receiving the information (even if this is part of the same international company) which guarantees the same degree of protection for employees.

11. Outsourced HRIS, payrolls or employee benefit providers

Contracts with providers must be amended to ensure that the provider undertakes to comply with the Act.

Organisations need to check that the servers used by their in-house or outsourced service providers are physically situated in South Africa, otherwise the section above will become relevant.

12. References

It could be argued that the Act prevents the supply of personal information to a potential employer as part of a reference checking process. However, if the employee (or ex-employee) has consented, then the reference may be given (ensuring that it is accurate). There is also a public interest defence in the Act, so, arguably, information in the public interest could be passed on.

It is recommended that application forms contain a clause requesting consent of the applicant to references being taken. To ensure openness and fairness, the clause should provide for the name of the potential referee to be known to and agreed by the applicant.

13. Employment Practices Code

In due course an employment practices Code may be issued as provided for in the Act.

Its purpose would be to strike a balance between the legitimate expectations of workers that personal information about them will be handled properly and the legitimate interest of employers in deciding how best, within the law, to run their business. It would address the impact of data laws on the employment relationship and would most probably contain provisions on the obtaining of information about employees, the retention of records, access to records and disclosure etc.

Employers will no doubt collect and keep information on any individual who might wish to work, works for or has worked for it. This could include applicants for employment, employees, casual staff contract staff, etc. Such information about individuals may be stored on a computer or in manual files.

Some examples of personal information likely to be covered in terms of the Act would include, but would not be limited to, the following:

- details of an employee salary and bank account held on the computer system;
- an email about an incident involving a named employee;
- a manager's report containing information on an employee where there is an intention for the information to be placed in the personnel file;
- an individual employee's personnel file with the specific-sub dividers identifying various information on the employee, such as leave details, performance reviews etc;
- application forms for a particular vacancy.

Examples of information which would be unlikely to be covered would include the following:

- information on the entire workforce's salary structure given by grade where individuals are not named and are not identifiable;
- a report on the comparative success of different recruitment campaigns where no details regarding individuals are held;
- a report on the results of "exit interviews" where all responses are anonymised and where the results are impossible to trace back to individuals;

The special personal information that may be processed about employees would include the following:

- information about their physical or mental health, which forms part of sickness records or obtained as part of a pre-employment medical questionnaire or examination and or drug or alcohol test results;
- criminal convictions in order to assess an employee suitability for certain types or positions of employment;
- disabilities and racial/gender origin in ensuring equality of opportunity and in order to ensure that recruitment processes do not discriminate.

14. Conclusion

We recommend that HR practitioners consult with their in-house or outsourced HRIS and/or payroll experts and labour law experts and jointly prepare a plan of action to ensure compliance with the Act. Communication with employees and employee representatives will be important to explain what, if any, changes in HR processes will be required and to assure them of the employer's intention to be fully compliant with the Act.

Not only does the employer have obligations and responsibilities in terms of the Act its managers, line managers and/or supervisors are also required to act responsibly in terms of the type of personal information that they may collected, used, disclosed or otherwise processed.

The provisions of the Act will impact on recruitment and selection procedures and policies as personal information will be processed regarding job applicants and pre-employment vetting. Recruitment and selection procedures and policies will need to comply with the provisions of the Act in relation to the retention of information, background checks, the extent of the information requested, disclosure of what information has been processed in making a decision and the consequences to the individual of not consenting to the processing of personal information in the recruitment and selection process.

Employers will need to ensure that policies and procedures are put in place in relation to its employment records. How will such information be collected, stored? What are the procedures in terms of disclosing such information and when and how will such records be deleted, the retention of information, the security of information held and the procedures for individual participation in accessing, correcting and/or the deletion of such records will need to addressed in detail in such policies and procedures.

Employers will also need to consider its monitoring policies in relation to its employee's use of its IT systems, telephones, emails and other company equipment such as vehicles. The monitoring policies that are in place will need to be audited to ensure that they comply with the provisions of the Act in relation to the retention of records of employees telephone calls for training, keeping a log of websites visited, CCTV monitoring in relation to safety and health compliance or to prevent theft and fraud.

The impact and implications are vast and resources with the required expertise should be approached to assist in ensuring compliance.

THIS FACT SHEET IS BASED ON THE WORK OF KERRY GANTLEY, PARTNER, OF COWAN HARPER ATTORNEYS. HER CONTRIBUTION IS GRATEFULLY ACKNOWLEDGED. THE FACT SHEET WAS REVIEWED BY YOLANDI ESTERHUIZEN (LEGISLATION MANAGER, SAGE VIP) AND ROB BOTHMA (BUSINESS CONNEXION). OUR THANKS TO THEM ALSO.

Kerry may be contacted on kgantley@chlegal.co.za.

SABPP FACT SHEET SERIES

Date	No	Subject
2013		
February	1	GAINING HR QUALIFICATIONS
March	2	ETHICS, FRAUD AND CORRUPTION
April	3	NATIONAL DEVELOPMENT PLAN
May	4	BARGAINING COUNCILS
June	5	EMPLOYMENT EQUITY
July	6	HR COMPETENCIES
August	7	HR MANAGEMENT STANDARDS
September	8	PAY EQUITY
October	9	COACHING AND MENTORING
November	10	HIV/AIDS IN THE WORKPLACE
2014		
February	1	EMPLOYING FIRST-TIME JOB MARKET ENTRANTS
March	2	PROTECTION OF PERSONAL INFORMATION ACT