The Protection of Personal Information Act in the Workplace – Good practice recommendations on employment practices

The Information Regulator has indicated to the author that it plans to make the Protection of Personal Information Act ("POPIA") effective before 31 March 2020. When effective, POPIA will apply to all public and private organisations, and to the personal information of all employees of such organisations. What does this mean for people practitioners? Due to the close relationship between employer and employees and the special duties owed between them, particular employee information protection issues arise in the employment context. It is important for organisations to process employee information in accordance with the POPIA in order to protect and promote the trust relationship between employee and employer. While many organisations have been working to ensure compliance with respect to their customer and vendor information, one important area that must not be overlooked is the POPIA's application to employee/HR information. The basic legal rules on protecting personal information and employment data are set out in the POPIA – the main legislation governing the collection, processing and distribution of personal data in South Africa.

So what is personal information or employee information? Quite simply, it is an employee's application file, personal file, payroll information, leave/medical file, and all the information employers have about their employee. In other words, anything that employer collects that contains an employee's personal information. It also extends to information regarding contractors, temporary staff, casual staff, interns etc. For ease of reference I will just refer to employee information.

Personal information is broadly defined under the POPIA and includes any information relating to an identified or identifiable person who can be identified by reference to such things as race, gender, sex, marital status, nationality, ethnicity, sexual orientation, physical or mental health, disability, religion, culture, language, education, medical, financial, biometric, criminal or employment information, identifying number, symbol, e-mail address, location, opinions, confidential correspondence etc.
As for "processing" employee information, that term is also broadly defined and includes collecting, receiving, recording, organising, collating, storing, updating or modification, retrieval, alteration, consultation or use. Basically, if your organisation collects any employee information (and it does) it is a processor, and is called a "Responsible Party" in the POPIA. The POPIA applies to the processing of employee information in the Republic, as well as when transferring such information cross-border.

An Employer must process employee information lawfully. In order to do this, it needs to comply with the 8 conditions set out in the POPIA. These conditions are[1]:

accountability (the employer is accountable for compliance with POPIA);
processing limitation (employee information must be processed lawfully (legal basis) and must be adequate, relevant and not excessive);
purpose specification (employee information must be collected for a specific, explicitly defined and lawful purpose. Employment information should not be retained any longer than is necessary for achieving the purpose);
further processing limitation (further processing must be compatible with the purpose of collection);
information quality (employer must take reasonably practical steps to ensure employee information is complete, accurate, not misleading and updated where necessary);
openness (what will the employee information be used for, who will it be shared with, will it go cross border etc.);
security safeguards (employer must take appropriate, reasonable technical and organisational measures to prevent:
loss of, damage to or unauthorised destruction of employee information;
unlawful access to or processing of employee information.
employee participation (access, correction, deletion).

An employee has the right to have his or her employee information processed in accordance with the 8 conditions for the lawful processing of personal information including the right:

to be notified that:
employee information about him or her is being collected; or
his or her employee information has been accessed or acquired by any unauthorised person;
to establish what employee information the Employer holds about him or her, and to request access to such information; and
to request, where necessary, the correction, destruction or deletion of his or her information (there are limitations).

One of the fundamental principles of the POPIA is that an employee must consent to the processing of employee information. Consent requires that the employee be fully informed of the nature and scope of the processing, including understanding fully how the information will be processed, used, and transferred to other entities. The consent must be voluntary, specific and informed. It is important that an employer not use its "unequal negotiation power" to gain consent from employees as this will not meet the definition of consent in terms of POPIA.

Without consent, there are only a number of other ways an employer can process employee information legally. Processing may only happen if:

the processing is necessary to conclude or perform in terms of the employment contract;
the processing is necessary to comply with legal obligations;
the processing protects the legitimate interests of the employee; or
the processing is necessary for pursuing the legitimate interests of the Employer.

Under the POPIA there is “special personal information”. Such information includes employee information revealing religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life, criminal behaviour or biometric information. Processing of such information is strictly prohibited unless certain exceptions are met. Each type of special personal information has its own exceptions, and special regard has to be taken of these in employment practices.

Areas of application for the 8 conditions for the lawful processing of employee information that should be of specific interest to all people practioners are:

recruitment and selection;
employment records;
monitoring employees at work;
information about employee’s health (including medical examinations and substance testing); and
trans-border information flows.

The recruitment and pre-employment checks can be intrusive. An employer should be open about its processes and must not collect more information than it needs at each stage of the recruitment process. The employer must also not retain information longer than is necessary, and must comply with rules about criminal convictions.

An employer will unavoidably handle data coming within the ‘special’ categories of personal information, i.e. sensitive employee information (e.g. employee illness information or administering employee benefits). This can usually only be done with explicit and freely-given consent.

Many employers monitor emails, IT equipment or have workplace CCTV. This is permitted if justified and the employer has a legal basis to do so (e.g. a legal obligation), but an employer should inform its employees that it does this. Covert surveillance is especially intrusive and can only be used in extreme cases and on a limited basis.

All health information is, in principle, private and there should be a clear basis for collecting or processing it. Health information must be kept particularly secure. Transfer of data outside the Republic requires special safeguards to be in place.

An employer should place special importance on protecting its employee’s personal information and only processing it in a lawful manner. This will help in cementing the trust relationship between employer and employee. How can an employer expect an employee to treat vendor and client personal information in such a manner if it does not do this with the employee information under its own control and possession?

Don’t Miss Steps

Ensure people practioners are part of the POPIA compliance discussion. POPIA compliance is a team effort and people practioners should play a critical component of that role.

Determine what personal and/or sensitive information on employees you have and determine what you

are using it for and where that information is located/stored.
Conduct an employee information impact assessment.
If you don't have consent determine what legitimate basis you have to process information, and if it is because of the employer's "legitimate interest" ensure you have documented the balancing of the employer's legitimate interest against the employees' privacy rights.
Notify employees of the nature and scope of processing and gain consent to the extent any employee data is being processed for any reason other than one based on a legitimate basis.
Ensure employees are informed of their rights regarding their information and ensure internal policies and procedures are in place to allow employees to exercise these rights and to monitor compliance going forward.
Ensure policies and mechanisms are put in place to ensure future compliance as the POPIA is not a one-and-done deal. Employers must continue to stay in compliance as new employees enter the workforce, as employees leave the workforce, and as new data containing protected information is produced, collected, stored, transferred, etc

While this short article certainly does not cover everything an employer needs to know about employee information and the POPIA, it is a good starting point and can assist you in structuring a more in-depth conversation with a personal information expert such as Lambert Legal Consulting SA (Pty) Ltd.

[1] *These conditions apply to all personal information including that of an employers clients and vendors.*