LARSON FALCONER HASSAN PARSEE INCORPORATED (LFHP)

RISK MANAGEMENT AND COMPLIANCE GUIDE IN RESPECT OF THE PROTECTION OF PERSONAL INFORMATION ACT, NO. 4 OF 2013

THE "POLICY"

THE PROTECTION OF PERSONAL INFORMATION ACT ("POPI")

Introduction

THE OBJECT OF THE ACT

CONSONANT with the Constitutional values of democracy and openness within the framework of the information, society requires the removal of unnecessary impediments to the free flow of information and regulate, in harmony with international standards, the Act seeks to:

(a) promote the protection of personal information processed by public and private bodies;
(b) introduce certain conditions to establish minimum requirements for the processing of personal information;
(c) establish an information regulator to exercise certain powers and to perform certain duties and functions in terms of the act;
(d) promote access to information
(e) issue codes of conduct to regulate conduct to conform with the act;
(f) to provide for rights of persons providing unsolicited electronic communications and automated decision making;
(g) to regulate the flow of personal information across the borders of the Republic.

KEY DEFINITIONS APPLICABLE TO LFHP

SECTION 1

''personal information'' means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to—

(a) information relating to the race, gender, sex, pregnancy, marital status, nationality, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;

(b) information relating to the education or the medical, financial, criminal or employment history of the person;

(c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other assignment to the person;

(d) the biometric information of the person;

(e) the personal opinions, views or preferences of the person;

(f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;

(g) the views or opinions of another individual about the person; and

(h) the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person;

"private body" means –

(a) a natural person that carries on any trade, business or profession ……;

(b) a partnership which carries on or carried on any trade, business or profession;

(c) a juristic person.

"record" means a recorded information –

(a) regardless of form or medium and includes:

(i) someone writing on any material;

(ii) information, produced, recorded or stored by means of any, … computer equipment, whether hardware or software or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored;

(iii) label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means;

(iv) book, map, plan, graph or drawing;

(v) photograph, film, negative, tape or other device in which one or more visual images are embodied to be capable, with or without the aid of some other equipment of being reproduced;

(b) in the possession or under control of a responsible party;

(c) whether or not it was created by a responsible party; and

(d) regardless of when it came into existence.

''responsible party'' means a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information;

PURPOSE OF ACT

SECTION 2

The purpose of this Act is to—

(a) give effect to the constitutional right to privacy, by safeguarding personal information when processed by a responsible party, subject to justifiable limitations that are aimed at—

(i) balancing the right to privacy against other rights, particularly the right of access to information; and

(ii) protecting important interests, including the free flow of information within the Republic and across international borders;

(b) regulate the manner in which personal information may be processed, by establishing conditions, in harmony with international standards, that prescribe the minimum threshold requirements for the lawful processing of personal information;

(c) provide persons with rights and remedies to protect their personal information from processing that is not in accordance with this Act; and

(d) establish voluntary and compulsory measures, including the establishment of an Information Regulator, to ensure respect for and to promote, enforce and fulfil the rights protected by this Act.

Application Provisions

APPLICATION AND INTERPRETATION OF THE ACT

SECTION 3

The act applies to personal information that has been entered in a record by or for a responsible party by making use of automated or non-automated means. Where the responsible party is domiciled within the Republic or makes use of automated or non-automated means in the Republic UNLESS those means are used only to forward personal information through the Republic.

"Automated means" any equipment capable of operating automatically in response to instructions given for the purposes of processing information.

APPLICATION TO LFHP

LFHP is an incorporated company duly registered in terms with the company laws of South Africa and registered with the Legal Practice Council as a firm of attorneys. LFHP is a responsible party which collects personal information within the meaning of these terms contemplated in section 1 of POPI, and, is accordingly obliged to comply with the provisions of POPI.

POPI requires LFHP to inform their clients and employees as to the manner in which their personal information is used, disclosed and destroyed. POPI requires LFHP to guarantee, commit to, protect its clients and employees privacy and ensure that their personal information is used appropriately, transparently, securely and in accordance with the appropriate applicable laws.

This Policy sets out the manner in which LFHP deals with its client and employee's personal information as well the purpose for which said information is used. LFHP has made this Policy made available on its website.

Nature of and definition of Data Subject in relation to LFHP

RIGHTS OF DATA SUBJECT

SECTION 5

Data subject is the person providing personal information and the data subject has certain rights which include:

(a) to be informed that personal information is being collected and for what purpose in terms of Section 18;

(b) if the personal information has been accessed by an unauthorised person in terms of Section 22;

(c) a right to access the full record of personal information by the responsible party in terms of Section 23;

(d) correct, destroy or delete personal information held in terms of Section 24;

(e) object to the processing of personal information in terms of Section 11(3)(a);

(f) object to the processing of personal information for the purposes of direct marketing in terms of Section 11(3)(b);

(g) object to the timeous proper notification of the right to use material for direct marketing in terms of Section 69(3);

(h) not to have personal information accessed for the purpose of direct marketing by means of unsolicited electronic means in terms of Section 69;

(i) not be subject to a decision based solely on automated processing of personal information intended to provide a profile other than for the purposes for which the personal information was intended in terms of Section 71 i.e. for the profiling of any performance at work, credit worthiness, reliability, location, health, personal preferences or conduct;

(j) submit a complaint with the Regulator for any alleged interference with the protection of personal information in terms of Section 74;

(k) institute civil proceedings for any infringement of personal information in terms of Section 99.

DATA SUBJECTS APPLICABLE TO LFHP

LFHP collects and processes clients and employees personal information pertaining to the their relationship with LFHP. LFHP also collects employee's personal information pertaining to the employee's employment contract.

The type of information collected will depend on the need for which it is collected and will be processed for that purpose only. Whenever possible, LFHP will inform the data subject what part of the information collected is required and what informational collected is optional.

TYPES OF INFORMATION ACCESSED BY LFHP

- A client's identity number, name, surname, address, postal code, marital status, and number of dependants;
- Description of a client's residence, business, assets, financial information, banking details, etc;
- Any other information required including clients suppliers and insurers in order to provide clients with an accurate analysis of their legal needs; and
- Information in respect of employees as required in terms of the various acts that govern employees, e.g., Compensation for Injuries and Diseases Act, Basic Conditions of Employment Act, Employment Equity Act, Labour Relations Act, Unemployment Insurance Act, Tax Administration Act and the Income Tax Act.

LFHP strives to ensure that the personal information accessed will be dealt with uniformly with all its associates and suppliers.

With the client's consent, LFHP may also supplement the information provided by information LFHP receives from other providers in order to offer a more consistent and personalized experience in the client's interaction with LFHP.

For purposes of this Policy, clients include potential and existing clients.

Processing Limitations

LAWFULNESS OF PROCESSING

SECTION 9

Personal information must be processed:

(a) lawfully; and

(b) in a reasonable manner that does not infringe the privacy of the data subject.

MINIMALITY

SECTION 10

Personal information may only be processed if it is adequate, relevant and not excessive.

CONSENT, JUSTIFICATION AND OBJECTION

SECTION 11

(1) Personal information may only be processed if—

(a) the data subject or a competent person where the data subject is a child consents to the processing;

(b) processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is party;

(c) processing complies with an obligation imposed by law on the responsible party;

(d) processing protects a legitimate interest of the data subject;

(e) processing is necessary for the proper performance of public law duty;

(f) processing is necessary for the purpose of legitimate interest of the responsible party or of a third party to whom the information is supplied;

(g) Responsible party bears the burden of proof that the data subject or competent person's consent is required for the processing of personal information;

(h) the data subject or competent person may withdraw his or her consent;

(i) the data subject may object to the processing of personal information on the following grounds:

(i) that there are reasonable grounds relating to his or her particular situation;

(ii) for the purposes of direct marketing;

(iii) once the data subject has objected and such objection is valid the responsible party may no longer process the information.

COLLECTION DIRECTLY FROM DATA SUBJECT

SECTION 12

(a) Personal information must be collected directly from the data subject;

(b) it's not necessary to comply with the provision that personal information must be collected directly from the data subject if:

(i) the information can be derived from a public record or is deliberately been made public by the data subject;

(ii) the data subject or competent person where the data subject is a child has consented to the collection of the information from another source;

(iii) the purpose of which is the prevention, detection, including assistance in the identification of proceeds of unlawful activities and the combating money laundering activities, investigation or proof of offences, the prosecution of offenders or the execution of sentences or security measures, to the extent that adequate safeguards have been established in legislation for the protection of such personal information.

(c) the collection of personal information will not prejudice the legitimate interest of the data subject;

(d) the collection of information from another source is necessary to:

(i) avoid prejudice to the maintenance of the law by any public body;

(ii) to enable compliance with an obligation imposed by the law enforcement agencies concerning the collection of revenue by the Revenue Services;

(iii) conduct of proceeding in any court;

(iv) interests of national security;

(v) to maintain the legitimate interests of the responsible party or third party to whom information is supplied.

(e) compliance would prejudice a lawful purpose of collection;

(f) is not reasonably practical in the circumstances of the particular case.

COLLECTION FOR SPECIFIC PURPOSE

SECTION 13

(a) personal information must be collected for a specific, explicitly defined and lawful purpose related to a function or activity of the responsible party;

(b) steps must be taken in accordance with Section 18(1) to ensure that the data subject is aware of the purpose of the collection of the information unless the provisions of Section (18)(4) are applicable.

APPLICATION TO LFHP

Consent to process client information shall be obtained from clients (or a person who has been given authorisation from the client to provide the client's personal information) during the introductory, appointment and the ongoing stage of the relationship. LFHP will complete Checklist 1 (as annexed hereto) and will ensure that the documents are completed in the presence of the data subject and signed by a LFHP representative as well as the data subject contemporaneously.

LFHP will only use the personal information accessed for lawful purposes as provided for in sections 10 and 11 of POPI which may include:

- providing products or services to clients and to carry out the transactions requested;
- assessing and processing the instruction according to the client's mandate;
- conducting credit reference searches or- verification;
- confirming, verifying and updating or correcting client details;
- for purposes of legal services rendered by the responsible party;
- for the detection and prevention of fraud, crime, money laundering or other malpractices as required by legislation;
- for audit and record keeping purposes;
- in connection with legal proceedings;
- providing LFHP services to clients, to render the services requested and to maintain and constantly improve the relationship;
- providing communication in respect of services and regulatory matters that may affect clients; and
- in connection with and to comply with legal and regulatory requirements or when it is otherwise allowed by law.

Accordingly, personal information may only be processed if certain conditions, listed below, are met along with supporting information (which includes consents, authorities or written agreements to evidence that the conditions have been met) for LFHP's processing of personal information:

- the client's consents to the processing - consent is obtained from clients during the introductory, appointment and other stages of the relationship;

- the necessity of processing - in order to conduct an accurate analysis of the client's needs for purposes of amongst others rendering legal services in terms of the client's mandate;
- processing complies with an obligation imposed by law on LFHP;

LFHP will not be required to retrospectively obtain consent for personal information collected prior to the application of the Act, save for instances where personal information collected is used for purposes other than for which it was originally intended.

Retention and Restriction of Records

SECTION 14

(a) records of personal information must not be retained for a period longer than is necessary for achieving the purpose for which the information was collected or subsequently processed;

(b) where the responsible party has used a record of personal information to decide then such record must be kept for a period:

(i) as maybe required or prescribed by law;

(ii) if there is no law then for a period that will afford the data subject a reasonable opportunity taking into consideration the purpose for which the data subject may require access to the record;

(iii) a responsible party must destroy or delete a record of personal information or de-identify the information as soon as its reasonable practical after the responsible party is no longer authorised to retain the record.

QUALITY OF INFORMATION

SECTION 16

(a) a responsible person must take reasonable practicable steps to ensure that the personal information is complete, accurate, not misleading and updated where necessary;

(b) processing personal information must be done having regard for the purpose of which this information is collected or further processed.

DOCUMENTATION

SECTION 17

A responsible party must maintain the documentation of all processing operations under its responsibility for the purposes of Promotion of Access to Information Act.

APPLICATION TO LFHP

Storage and security of personal information

LFHP will continuously review its security controls and processes to ensure that personal information is secure.

The following procedures are in place in order to protect personal information:

- LFHP has appointed Reeves Parsee as an Information Officer who is responsible for the compliance with the conditions of the lawful processing of personal information and other provisions of POPI;
- this Policy has been put in place and training on this Policy and the POPI Act has already taken place and will be conducted regularly by LFHP compliance personnel;
- each new employee will be required to sign an employment contract containing relevant consent clauses for the use and storage of employee information, also

for the instances of loss, correction and destruction of the personal information or any other action so required, in terms of POPI;

- every employee currently employed by LFHP will be required to sign an addendum to their employment contracts containing relevant consent clauses for the use and storage of employee information, or also for the instances of loss, correction and destruction of the personal information any other action so required, in terms of POPI;
- LFHP archived client information is stored on site and access to these areas is limited to authorized personnel;
- LFHP product suppliers, insurers and other third-party service providers will be required to sign a service level agreement guaranteeing their commitment to POPI; and
- all electronic files or data are backed up by LFHP's IT department which is also responsible for system security that protects third party access and physical threats. The IT department is also responsible for electronic information security.

Destruction of Documents

Documents may be destroyed after the termination of the retention period. Departments will be requested to attend to the destruction of their documents and these requests shall be attended to as soon as possible, after legal requirements have been met.

Files must be checked in order to make sure that they may be destroyed and also to ascertain if there are important original documents in the file. Original documents must be returned to the holder thereof, failing which, they should be retained by LFHP pending such return.

After completion of the process detailed above, the Director of a department shall, in writing, authorise the removal and destruction of the documents in the authorisation document. These records will be retained by the Information Officer.

The documents are then made available for collection by the removers of LFHP's documents, who also ensure that the documents are shredded before disposal. This also helps to ensure confidentiality of information.

Documents may also be stored off-site, in storage facilities approved by LFHP.

Notification to Data Subject when collecting personal information

SECTION 18

The responsible party must take reasonable practical steps to ensure that the data subject is aware of the following, (as per check list 2):

(a) the information being collected that where the information is not collected from the data subject, the source from which it is collected;

(b) the name and address of the responsible party;

(c) the purpose for which the information is being collected;

(e) whether or not the supply of information by that data subject is voluntary or mandatory;

(f) any particular law authorising or requiring the collection of the information;

(g) the responsible person intends to transfer information to the third country or international organisation and the level of protection afforded to the information by that third country or international origination;

(h) any further information such as:

  (i) recipient or category of recipients of the information;

  (ii) nature or category of the information;

  (iii) existence of the right of access to and the right to rectify the information collected;

  (iv) existence of the right of object to the processing of personal information as referred to in section 11(3);

  (v) right to lodge a complaint to the Information Regulator and the contact details of the Information Regulator;

APPLICATION TO LFHP

LFHP shall ensure that Checklist 1 and Checklist 2 (as annexed hereto) are completed in the presence of a data subject and signed by a representative of LFHP and the data subject each time personal information is collected from a data subject.

Security Measure on Integrity and Confidentiality of Personal Information

SECTION 19

(a) Security measures on integrity and confidentiality of personal information it has processed and in doing so must prevent:

  (i) loss of, damage to or unauthorised destruction of personal information; and

  (ii) unlawful access to or processing of personal information.

(b) In order to ensure integrity and confidentiality the responsible party must take reasonable measures to:

  (i) identify reasonably foreseeable internal and external risks to personal information;

  (ii) establish and maintain appropriate safeguards against the risks identified;

  (iii) regularly verify that the safeguards are effectively implemented; and

  (iv) ensure that the safeguards are continually updated to respond to new risks or Deficiencies.

(c) The responsible party must have due regard to generally accepted information security practices and procedures that is necessary to its specific industry or professional rules and regulations of specific industry or professional rules and regulations.

INFORMATION PROCESSED BY OPERATOR OR PERSON ACTING UNDER AUTHORITY

SECTION 20

An operator or anyone processing personal information on behalf of a responsible party or an operator, must:

(a) process such information only with the knowledge or authorisation of the responsible party; and

(b) 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.

SECURITY MEASURES REGARDING INFORMATION PROCESSED BY OPERATOR

SECTION 21

(1) A responsible party must, in terms of a written contract between the responsible party and the operator, ensure that the operator which processes personal information for the responsible party establishes and maintains the security measures referred to in section 19.

(2) The operator must notify the responsible party immediately where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person.

NOTIFICATION OF SECURITY COMPROMISES

SECTION 22

(1) Where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person, the responsible party must notify—

(a) the Regulator; and

(b) subject to subsection (3), the data subject, unless the identity of such data subject cannot be established.

(2) The notification referred to in subsection (1) must be made as soon as reasonably possible after the discovery of the compromise, taking into account the legitimate needs of law enforcement or any measures reasonably necessary to determine the scope of the compromise and to restore the integrity of the responsible party's information system.

(3) The responsible party may only delay notification of the data subject if a public body responsible for the prevention, detection or investigation of offences or the Regulator determines that notification will impede a criminal investigation by the public body concerned.

(4) The notification to a data subject referred to in subsection (1) must be in writing and communicated to the data subject in at least one of the following ways:

(a) Mailed to the data subject's last known physical or postal address;

(b) sent by e-mail to the data subject's last known e-mail address;

(c) placed in a prominent position on the website of the responsible party;

(d) published in the news media; or

(e) as may be directed by the Regulator.

(5) The notification referred to in subsection (1) must provide sufficient information to allow the data subject to take protective measures against the potential consequences of the compromise, including—

(a) a description of the possible consequences of the security compromise;

(b) a description of the measures that the responsible party intends to take or has taken to address the security compromise;

(c) a recommendation with regard to the measures to be taken by the data subject to mitigate the possible adverse effects of the security compromise; and

(d) if known to the responsible party, the identity of the unauthorised person who may have accessed or acquired the personal information.

(6) The Regulator may direct a responsible party to publicise, in any manner specified, the fact of any compromise to the integrity or confidentiality of personal information, if the Regulator has reasonable grounds to believe that such publicity would protect a data subject who may be affected by the compromise.

APPLICATION TO LFHP

Security of personal information

As set out above, LFHP has procedures in place to ensure the security and integrity of personal information collected.

Disclosure of personal information by LFHP

LFHP may disclose:

- a client's personal information to any of its, advocates, agents and or approved product- or third-party service providers whose services or products clients elect to use. LFHP has agreements in place with such service providers to ensure compliance with confidentiality and privacy conditions;
- personal information with, and obtain information about clients from third parties for the reasons already discussed above; and
- a client's information where it has a duty or a right to disclose in terms of applicable legislation, the law, or where it may be deemed necessary in order to protect LFHP's rights.

Unauthorised Access

In the event of any form of unauthorized access of a client's personal information LFHP shall:

- notify the client immediately;
- notify the Regulator;
- provide sufficient information about the unauthorized access, details of the entity or persons that have gained access;
- detail the possible risks;
- recommend measures to mitigate any risk; and
- seek the Regulators direction on any measures to mitigate the clients risk.

Data Subject Participation

ACCESS TO PERSONAL INFORMATION

SECTION 23

(1) A data subject is entitled to know, provided that he has adequately identified himself:

(a) whether or not the responsible party holds any of his personal information;

(b) a record or description of the personal information held by the responsible party or any other third party within:

(i) a reasonable time;

(ii) at a prescribed fee;

(iii) in and reasonable manner and format;

(iv) in a form generally understandable.

(c) to know that he can correct the personal information held;

(d) what fees he will need to pay to access the personal information or how much of the initial deposit or all or part thereof is payable.

APPLICATION TO LFHP

In terms of this section, clients have the right to access the personal information LFHP holds about them. Clients also have the right to ask LFHP to update, correct or delete their personal information on reasonable grounds. Once a client objects to the processing of their personal information, LFHP may no longer process said personal information. LFHP will take all reasonable steps to confirm its clients' identity before providing details of their personal information or making changes to their personal information.

The details of LFHP's Information Officer and Head Office are as follows:

- **Information Officer**

Name: S R PARSEE

Contact Number: 083 500 9621

Office Number: 031 534 1604

E-mail Address: Reeves.Parsee@lfhp.co.za

- **Deputy Information Officer**

Name: Sarah Stringer

Contact Number: 031 534 1605

E-mail Address: Sarah.Stringer@lfhp.co.za

Correction of personal information

SECTION 24

(1) the data subject may in a prescribed manner request:

(a) a correct or deletion of personal information that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully;

(b) request a destruction or deletion of the record of personal information that the responsible party is no longer authorised to retain in terms of Section 14

(2) on request for the correction or deletion the responsible party must do so:

(a) correcting the information;

(b) destroying or deleting the information;

(c) satisfactorily providing evidence of such destruction or deletion;

(d) where such agreement on destruction or deletion cannot be achieved the data subject's request for correction or deletion must be recorded and must be read with the information already supplied.

(3) if the responsible party has taken steps to correct or delete information and the effect of it is that it will affect the third parties such third parties must be notified of such changes;

(4) the data subject must be appraised of all steps taken by the responsible party in terms of its request.

APPLICATION TO LFHP

LFHP must ensure it complies with the steps set out above when correcting personal information on file.

Prohibition on processing of special personal information

SECTION 26

(1) responsible party may not process personal information concerning:

(a) religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of the data subject;

(b) the criminal behaviour of the data subject which relates to the alleged commission by the data subject of any offence or any proceedings in respect of any offence allegedly committed by the data subject.

(c) the prohibition does not apply if:

(i) the processing it carried out with the consent of the data subject;

(ii) processing is necessary for the establishment, exercise or defence of a right or obligation in law;

(iii) processing is necessary to comply with the obligation of international public law;

(d) processing is for historical, statistical or research purposes that serves a public interest or appears to be impossible or disproportionate to ask for consent provided that sufficient guarantees are provided for protecting any adverse consequences;

(e) information has been deliberately made by the data subject in public.

Access to documents

All LFHP and client information will be dealt with in the strictest confidence and may only be disclosed in any one of the following circumstances as per section 26 of the act:

- disclosure is under compulsion of any law;
- there is a duty to the public to disclose;
- the interests of LFHP require disclosure; or
- disclosure is made with the express or implied consent of the client.

AUTHORISATION CONCERNING DATA SUBJECT'S SEX LIFE

SECTION 32

(1) The prohibition concerning the subject's health or sex life does not apply to processing by:

(a) a medical professional, healthcare institutions or facilities or social services, if such processing is necessary for the proper treatment and care of the data subject or for the administration of the institute or professional practice concerned;

(b) insurance companies, medical schemes, medical scheme administrators and managed healthcare organisations that have to access risk, perform an insurance or medical scheme agreement or enforcement of any contractual rights and obligations ….

(c) administrative bodies, pension funds, employers or institutions working for them if such processing is necessary for, provisions of laws, pension regulations or collective agreements which create rights dependent on the health or the sex life of the data subject or reintegration of or support for workers or persons entitled to benefit in connection with sickness or work incapacity.

(2) the information may only be processed by responsible parties subject to an obligation of confidentiality.

(3) personal information concerning inherited characteristics may not be processed unless a serious medical interest prevails, or the processing is necessary for historical, statistical or research activity.

AUTHORISATION CONCERNING DATA SUBJECT'S CRIMINAL BEHAVIOUR

SECTION 33

(1) a data subject's criminal behaviour or biometric information may not be processed unless processing is carried out by bodies charged by law with applying criminal law or by responsible parties who have obtained that information in accordance with the law.

(2) be processed under the rules established in compliance with labour legislation.

(3) processing is necessary to supplement the processing of information on criminal behaviour or biometric information permitted by this section.

AUTHORISATION CONCERNING PERSONAL INFORMATION OF CHILDREN

SECTION 34

(1) the prohibition of processing of personal information of children does not apply if:

(a) carried out with prior consent of a competent person;

(b) necessary for the establishment, exercise of defence of right or obligation in law;

(c) necessary to comply with an obligation of international public law;

(d) for historical, statistical or research purposes provided that the said purposes are necessary in the public interest and it appears to be impossible or disproportionate to ask for consent however sufficient guarantees must be provided to ensure that processing does not adversely affect the individual privacy of a child;

(e) has been deliberately made public by the child or the consent of a competent person.

APPLICATION TO LFHP

LFHP shall not be entitled to process the personal information contemplated in section 26 of POPI unless such information falls within the ambit of the exceptions contemplated in sections 32 – 34.

Information Officer

DUTIES AND RESPONSIBILITIES OF INFORMATION OFFICER

SECTION 55

(1) an information officer's responsibilities include:

(a) the encouragement of compliance by the body with the conditions for the lawful processing of personal information;

(b) dealing with requests made to the body pursuant to the Act;

(c) working with the Regulator when investigations are being conducted;

(d) otherwise ensuring compliance by the body with the provisions of the Act;

It is to be noted that officer's must take up their duties in terms of this Act only after the responsible party has registered them with the Regulator.

Records that cannot be found

If LFHP searches for a record and it is believed that the record either does not exist or cannot be found, the requester will be notified by way of an affidavit or affirmation. This will include the steps that were taken the attempt to locate the record, the risks associated with such loss and the mitigation to be carried out by the client and LFHP's proposed mitigation measures as required by section 19 of POPI.

Designation and delegation of deputy Information Officers

SECTION 56

1. The responsible body must make provision for:

   (a) such number of persons, if any, as deputy information officers;

   (b) any power or duty conferred or imposed on any information officer by this Act to a deputy information officer of that body.

Direct marketing by means of unsolicited electronic communications

SECTION 69

(1) the process of personal information of a data subject for the purpose of direct marketing by means of any form of electronic communications, including automatic calling machines, facsimile machines, SMS's or e-mails is prohibited unless the data subject:

   (a) has given his, her or its consent to the processing; or

   (b) is a customer of the responsible party:

(2) a responsible party may approach the data subject:

   (a) whose consent is required;

   (b) who has not previously withheld such consent, only once in order to request the consent of the data subject.

   (c) the data subject's consent must be requested in the prescribed manner and form;

(3) a responsible party may only process the personal information of a data subject who is a customer of the responsible party:

   (a) if the responsible party has obtained the contact details of the data subject in the context of the sale of a product or service;

(b) for the purpose of direct marketing of the responsible party's own similar products or services; and

(c) if the data subject has been given a reasonable opportunity to object, free of charge and in a manner of un-necessary formality to such use of his or her electronic details:

(i) at the time when the information was collected

(ii) on the occasion of each communication with the data subject for the purpose of marketing if the data subject has not initially refused such use.

(4) any communication for the purpose of direct marketing must contain:

(a) details of the identity of the sender or the person on whose behalf the communication has been sent;

(b) the address or contact details to which the recipient may send a request that such communications cease.

"**Automatic calling machine"** means a machine that is able to do automated calls without human intervention.

Automated decision making

SECTION 71

(1) data subject may not be subject to a decision which results in legal consequences for him which is based solely on the basis of the automated processing of personal information intended to provide a profile of such person including his performance at work, credit worthiness, reliability, location, health, personal preferences or conduct

(2) the above prohibition does not apply if

(a) the parties have entered into contract and

(i) the request for data subject in terms of the contract has been met;

(ii) appropriate measures have been taken to protect the data subject's legitimate interests;

(b) is governed by law or code of conduct in which appropriate measures have been provided to protect the legitimate interest of the data subject.

(3) the appropriate measures referred to must

(a) provide an opportunity for the data subject to make representations about a decision referred to in Section 71 (1) ;

(b) require a responsible party to provide a data subject with sufficient information about the underlying logic of the automated processing of the information relating to the subject to enable him to make representations relating thereto.

Transfer of personal information outside the Republic

SECTION 72

(1) LFHP shall not transfer personal information about a data subject to a third party who is in a foreign country unless:

(a) it has complied with the provisions of Section 72 relating to trans-border information flows;

(b) The data subject consents to the transfer of personal information to a foreign country prior to transfer and obtains written consent of the data subject which may be in the form that the information Regulator may determine;

(c) even where the written consent of the data subject has been obtained, if the foreign country does not have adequate law protecting the personal information, that an agreement, which may be in the form the information Regulator may determine, has been concluded prior to the transfer of the personal information to the foreign country then only can the personal information be released.

Miscellaneous provisions to be noted by LFHP

ENFORCEMENT

SECTION 73

Section 73 to Section 98 deals with various rights of the Regulator to enforce the Act and provides technical information regarding the manner in which the Regulator is obliged to receive complaints, provide the responsible party with an opportunity to respond, to adjudicate the complaint and enforce the Act.

CIVIL REMEDIES

SECTION 99

(1) a data subject may institute civil action for damages in a court having jurisdiction against the responsible party for breach of any provision of the Act whether or not there is intent or neglect on the part of the responsible party;

(2) Responsible party may raise the following defences to any civil action, namely:

- (a) Vis major;
- (b) consent of the Plaintiff;
- (c) fault on the part of the Plaintiff;
- (d) compliance was not reasonably practicable in the circumstances of the particular case;
- (e) where the Regulator has granted the responsible party exemption.

(3) the court hearing the proceedings may award an amount that is just and equitable including:

- (a) payment of damages as compensation for patrimonial and non-patrimonial loss suffered by a data subject as a result of the breach;
- (b) aggravated damages in the sum determined in the discretion of the court;
- (c) interest and
- (d) costs of suite.

(4) any amount awarded by the Regulator has the effect of a civil judgment.

OFFENCES, PENALTIES AND ADMINISTRATIVE FINES

SECTION 100

(a) Section 101 to Section 107 provide that any person who contravenes the provisions of Section 54 relating to breach of confidentiality is guilty of an offence;

(b) a responsible party who fails to comply with enforcement notices served on them in terms of Section 95 is guilty of an offence;

(c) the credit Regulator may impose administrative fines which may not exceed R10 000 000.00 (ten million rands);

(e) if the infringer elects to be tried in a court on a charge of having committed alleged offences, the Regulator must hand this matter over to the South African Police Services and inform the infringer accordingly;

(f) if the infringer fails to comply with the requirements of the notice, the Regulator must file with the clerk or the registrar of the competent court a statement certified by it as correct setting forth the amount of administrative fines payable by the infringer and such statement thereupon has the effect of a civil judgment lawfully given in that court in favour of the Regulator for a liquidated debt;

(g) no prosecution may be instituted against a responsible party if the responsible party concerned has paid an administrative fine in terms of the Act;

(h) the administrative fine imposed in terms of this section does not constitute a previous conviction;

(i) all fines paid in terms of the Act must be paid to the National Revenue Fund.

Amendments to this Policy

Amendments to, or a review of this Policy, will take place on an *ad hoc* basis or at least once a year. Clients are advised to access LFHP's website periodically to keep abreast of any changes. Where material changes take place, clients will be notified directly, or changes will be stipulated on LFHP's website.