Axiomatic Consultants

Protection of Personal Information Policy

Introduction

Axiomatic because of the role it fulfils as collator and custodian of sensitive personal information has a legal and moral responsibility to both the company and employees to ensure that all members of the Axiomatic team:

- ✔ obtain and process personal information fairly; and
- ✔ keep it only for a specified and explicit lawful purpose; and
- ✔ process it only in ways compatible with the purposes for which it was given initially; and
- ✔ keep personal data safe, confidential and secure; and
- ✔ keep data accurate, complete and up-to-date; and
- ✔ retain it for a period no longer than is necessary for the specified purpose; and
- ✔ provide a copy of his/her personal information to any individual, on request.

The introduction of the Protection of Personal Information Act ("POPIA") further strengthens the need to ensure confidentiality of personal information. The POPIA is an important legal reform, creating a regime of consumer protection that has become essential in the information age. It is data protection legislation intended to protect individuals from other parties processing of information about them. The legislation centres on a set of 'information protection principles' which flesh out a general and higher-level requirement that personal information must be processed lawfully and 'in a reasonable manner that does not infringe the privacy of the data subject'

Three important concepts are defined in the Act namely:

'Data subject' means, according to the definitions in Section 1, the person to whom personal information relates. While the data subject is the principal right-holder under the POPIA, the principal duty-bearer is termed the 'responsible party', defined as 'the public or private body or any other entity which, alone or in conjunction with others, determines the purpose of and means for processing personal information'.

"personal information" means information about a person's race, gender, sex, pregnancy, marital status, nationality, ethnic or social origin, sexual orientation, age, physical or mental health, disability, religion, conscience, belief, culture, language, education, medical information, financial information, criminal or employment history, an identifying number, e-mail address, physical address, telephone number, blood type, biometric information, personal opinions, views or preferences of a person; correspondence of a private or confidential nature; and the name of the person if it appears with other personal information relating to the person.

"process" meaning collection, receipt, recording, organization, collation, storage, updating or modification, retrieval, alteration, consultation, use, dissemination, distribution, merging, linking, blocking, degradation, erasure or destruction of information.

POPIA requires that an Information Protection Officer be appointed. Brett Hopkins will assume the duties of the Information Protection Officer for the company where the responsibilities are defined in the Act as:

46. (1) Each responsible party must ensure that there are, within that body, one or more information protection officers whose responsibilities include -

(a) the encouragement of compliance, by the body, with the information protection principles;

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

(c) working with the Commission in relation to investigations conducted pursuant to Chapter 6 of this Act in relation to the body;

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

In information protection principles contained in POPIA can be summarised as follows:

- Any person who stores personal and private information ("PI") about anyone else may not do so without the direct consent by the effected person - the 'data subject'.
- Any 'data subject' may request to review any PI stored about them at any time and such information may not be withheld. The 'data subject' may request for corrections to be made to erroneous information and the data holder will be obliged to make such corrections.
- No PI may be disclosed to any person without the direct authorisation of the 'data subject'. A breach in this regard will be considered a serious and punishable offence.
- No alterations or changes of any nature may be made to the PI or data kept on a 'data subject' without the direct authorisation of the 'data subject'.
- No data may be released to any person resulting in the distinctive identification of a 'data subject' for the purposes of research, statistics or any other similar purpose.

It is therefore essential that Axiomatic employees working with the personal information of employees must be educated on the principles of POPIA and how to deal with requests by any person regarding enquiries regarding "data subjects'. The golden rule should be not to disclose any information to any person if you are not convinced it is correct to do so. In such an instance, the request should be forwarded to the Information Protection Officer.

Security measures regarding the protection of employee information must be reviewed in order to ensure the safe keeping of information

The purpose of this Policy is to provide guidelines to assist employees to ensure that PI in their possession is kept safe and secure and that Axiomatic therefore meets all legal responsibilities.

GENERAL PROCEDURES

This section of the Policy sets out guidelines in a number of specific areas where particular attention should be paid in order to help protect the confidentiality of PI held by IAS.

1. It is essential that the Information Protection Officer is aware of what PI is held, where it is held and the consequences should that PI be lost or stolen;

2. Access to the Axiomatic office as well as data centres and server rooms used to host hardware and software on which PI is stored should be restricted only to those Axiomatic staff members that have authorisation to view and access the PI;

3. Access to systems which are no longer in active use and which contain PI should be removed where such access is no longer necessary or cannot be justified;

4. Passwords used to access PCs, applications and databases should be of sufficient strength to deter password cracking or guessing attacks. A password should include numbers, symbols, upper and lowercase letters. If possible, password length should be around 12 to 14 characters but at the very minimum of 8 characters. Passwords based on repetition, dictionary words, letter or number sequences, usernames, or biographical information like names or dates must be avoided. The Protection Information Officer is responsible to ensure that passwords are changed on a regular basis and that an audit trail is received which highlights non compliance;

5. A procedure must be instituted which evaluates requests from other organisations or third parties for access to PI stored in Axiomatic;

6. Personnel who retire, transfer or resign should be removed immediately from mailing lists and access control lists. It is the responsibility of the Protection Information Officer to ensure that procedures are in place to ensure compliance with this provision of the Policy;

7. Contractors, temporary staff, consultants and external service providers employed by Axiomatic should be subject to strict procedures with regard to accessing PI. This must be by way of a formal contract which includes the necessary confidentiality clauses and ensures that such parties will undertake and adhere to similar requirements as set out in this Policy to ensure the confidentiality of PI;

8. The Protection Information Officer must ensure that each employee receives a copy of this Policy and the Axiomatic Telecommunications and Electronic Communications Policy. Both policies should be understood and signed by each employee of the Company;

9. The Protection Information Officer is responsible for completing a Risk Audit examining the risks associated with the storage, handling and protection of PI at least every six months;

10. Procedures should be put in place in relation to disposal of files (both paper and electronic) containing PI. Paper with PI must be shredded and the Protection Information Officer must ensure that adequate shredders are available. Further, procedures should also be put in place in relation to the secure disposal of computer equipment (especially storage media) at end-of-life;

11. New staff should be carefully coached, trained and should be fully informed of their obligations before being allowed to access confidential or PI;

12. Staff should ensure that visitors to the office or other unauthorised persons are unable to view personal or sensitive information whether held in the form of paper documents or information displayed on PC monitors;

13. All staff should ensure that PCs are logged off or 'locked' when left unattended for any period of time. Where possible, staff should be restricted from saving files to the local disk. Users should be instructed to only save files to their allocated network drive;

14. PI documents must be locked away in a secure location when not in use. A "Clean Desk Policy" must be implemented to ensure that no documentation is left on employee's desks overnight;

15. Appropriate and secure filing procedures (both paper and electronic) should be drawn up and followed.

PAPER RECORDS

The following guidelines should be followed with regard to PI data held on paper files:-

1. Paper records and files containing PI should be handled in such a way as to restrict access only to those persons with business reasons to access them;

2. This should entail the strict enforcement of a policy whereby paper files containing such data are locked away when not required or overnight – a "clean desk policy". Where possible, consideration should also be given to the implementation of a register or logging access to paper files containing PI;

4. PI held on paper must be kept hidden from visitors to the offices;

5. Secure disposal of confidential waste should be in place and properly used. The discipline must be instilled into all staff members that papers, notes or any paper containing PI must be shredded.

EMAIL

All members of Axiomatic staff are required to take extreme care when using email; in particular:

1. Standard unencrypted email should **never** be used to transmit any PI. Staff members that have to use email to transfer such data must ensure that PI is encrypted either through file encryption, the use of a secure email facility which will encrypt the data (including any attachments) being sent or at the very least, robust passwords. The default option should always be to utilise the strongest encryption methods available. Employees should ensure that emails contained PI is sent only to the intended recipient;

2. Where PI is held on applications and databases with relevant security and access controls in place, additional controls should be considered that would prevent such data from being copied to applications where no security or access controls are in place and/or can be bypassed.

REMOTE ACCESS

There is an increasing business requirement for mobile working and for Axiomatic staff to be able to access servers and databases from home or remotely. This brings its own challenges in relation to data security which Axiomatic must address. With regard to PI, the following guidelines should be adhered to:-

1. In the first instance, all PI held electronically should be stored centrally on the server. Data that is accessible by remote access should not be copied to employee's PCs or to portable storage devices, such as laptops, memory sticks and external hard drives that may be stolen or lost;

2. When accessing data remotely, it must be done via a secure encrypted link with relevant access controls in place;

3. Additional stringent security and access controls should be in place including inter alia, the mandatory use of strong passwords or security token authentication;

4. PI being accessed in this way should be prevented from being copied from the central location to the remote device;

5. Axiomatic will utilise technologies that will provide for the automatic deletion of temporary files which may be stored on remote machines by its operating system;

6. Axiomatic must ensure that only known machines configured appropriately to the Company's standards (for example with up-to-date anti-virus and anti-spyware software and full encryption), are allowed to remotely access centrally held PI. Authorisation for remote access must be furnished by the Protection Information Officer. The strongest encryption methods available should be used to encrypt data on these machines;

7. Staff should be aware that it is imperative that any wireless technologies or networks used when accessing Axiomatic's systems should be encrypted to the strongest standard available.

LAPTOPS AND OTHER MOBILE STORAGE DEVICES

(Including Mobile Phones, USB memory sticks and External Hard Drives)

The use of laptops, USB memory sticks and other portable or removable storage devices has increased substantially in the last number of years. Likewise, the use of mobile phones to access and send emails has also increased. These devices are useful business tools however they are highly susceptible to loss or theft and often contain inferior security protection. Concomitantly, to protect the content held on these devices, the following recommendations should be followed:

1. All portable devices should be password-protected to prevent unauthorised use of the device and access to PI held on the device. In the case of mobile phones, both a PIN and login password should be used. Manufacturer or operator-provided PIN codes must be changed from the default setting by the user on receipt of the device;

2. Passwords used on these devices should be of sufficient strength to deter password cracking or guessing attacks and conform to the requirements listed in 'General Procedures' above;

3. PI should not be stored on portable devices. In cases where this is unavoidable, all devices containing this type of data must be encrypted and password protected. With regard to laptops, full disk encryption must be employed regardless of the type of data stored;

4. When laptops or cell phones are being used in public places, care must be taken to avoid unwitting disclosure of PI;

5. Portable devices must not contain unauthorised, unlicensed or personally licensed software. All software must be authorised and procured through Axiomatic's IT Company;

6. Anti-virus/Anti-spyware/Personal Firewall software must be installed and kept up to date on portable devices. These devices should be subjected to regular virus checks using this software;

7. Axiomatic must ensure that when providing portable devices for use by staff members, each device is authorised for use only by a specific named individual. The responsibility for the physical safeguarding of the device will then rest with that individual;

8. Laptops must be physically secured if left in the office overnight. When out of the office, the device should be kept secure at all times;

9. Portable devices should never be left in an unattended vehicle. Further, a policy must be introduced and strictly adhered to that if a member of staff is going out after work and the laptop will have to be kept in the car, then the laptop must be locked in a secure place in Axiomatic's office overnight;

10. Portable storage media should only be used for data transfer where there is a business requirement to do so;

11. Staff owned devices including portable media players such as iPods, digital cameras, and USB sticks must be technologically restricted from connecting to Axiomatic computers;

12. A robust, clear and known procedure for early notification of the loss of a portable device must be instituted. This would allow for the disconnection of the missing device from the Company's server;

DATA TRANSFERS OF PERSONAL INFORMATION

Data Transfers are a daily business requirement when transferring PI, such transfers should take place only where absolutely necessary and employing the most secure channel available. To support this, all members of Axiomatic must adhere to the following:-

1. Data transfers should, where possible, only take place via secure on-line channels where the data is encrypted

2. 'Strong' passwords (see 'General Procedures') must be used to protect the data during transfer. Such passwords must not be sent with the data it is intended to protect. Care should be taken to ensure that the password is sent securely to the intended recipient and that it is not disclosed to any other person;

3. Standard email should never be used to transmit any personal data. Where file encryption or the use of a ***secure email*** facility which will encrypt the data (including any attachments) is sent, staff must still ensure that the mail is sent only to the intended recipient.

4. When a data transfer with a third party is required, a written agreement should be put in place between both parties in advance of any data transfer. Such an agreement should define:-

   - The information that is required by the third party and the purposes for which the information can be used must also be defined if the recipient party is carrying out processing on behalf of Axiomatic;
   - Named contacts in each organisation responsible for the data;
   - The frequency of the proposed transfers;
   - An explanation of the requirement for the PI or requested data transfer;
   - The transfer and encryption method that will be used (e.g. Secure FTP, Secure email, etc.);
   - The acknowledgement procedures on receipt of the PI;
   - The length of time the information will be retained by the third party;
   - Confirmation from the third party that the security, confidentiality and storage of the PI will be handled to the same level of controls that Axiomatic would apply to that category of information. Confirmation is also required clearly identifying the point at which the third party will take over responsibility for protecting the data.
   - The method for highlighting breaches in the transfer process;
   - Business procedures need to be in place to ensure that all such transfers are legal, justifiable, necessary of not contrary to any legislation requirement or provision;

5. Given that Axiomatic operates globally, all staff members need to be aware of the stipulations pertaining to transferring PI of a data subject to a third party who is in a foreign country. Transfers of PI to a foreign country will be banned unless permission is granted by the Information Protection Officer or unless:

   - The recipient is subject to a law, binding code of conduct or binding agreement which upholds POPIA principles and is substantially similar.
   - Includes provisions substantially similar to this section.

- The data subject's consent.
- The transfer is necessary for performance of a contract between the data subject and the responsible party or for the implementation of pre-contractual measures.
- The transfer is necessary for the conclusion or performance of a contract between responsible party and third party that is in the interest of the data subject.
- The transfer is for the benefit of the data subject and it is not reasonably practicable to obtain consent.
- It is likely that the data subject would give consent.

REQUEST FOR ACCESS TO PERSONAL INFORMATION

Section 22 of the POPIA states that a data subject may request a responsible party to confirm that they are holding PI about the data subject and may obtain a description of that information and details about who has had access to it. Where such a request is received, the matter must be referred to the Information Protection Officer who will ensure that the correct procedures are adopted.

Section 23 of the POPIA, provides for a right to request correction of personal information held by a responsible party if it is inaccurate, incomplete, misleading, out of date, and obtained unlawfully, irrelevant or excessive. Where such a request is received, the matter must be referred to the Information Protection Officer who will ensure that the correct procedures are adopted.

APPROPRIATE ACCESS AND AUDIT TRAIL MONITORING

Axiomatic have an obligation to keep information safe and secure and have appropriate measures in place to prevent unauthorised access to, or alteration, disclosure or destruction of, the PI and against their accidental loss or destruction. It is imperative therefore, that Axiomatic have security in place to ensure that only those staff members with a business need to access particular PI are allowed to access the data. In addition to this general requirement, the following guidelines should be adopted:

1. Axiomatic must ensure that their ICT systems are protected by use of appropriate firewall technologies and that this technology is kept up-to-date and is sufficient to meet emerging threats. The monitoring of the suitability of such safeguards will be the responsibility of the Information Protection Officer;

2. In order to capture instances of inappropriate access (whether internal or external), addition, deletion and editing of data, audit trails should be used;

3. Access to files containing PI should be monitored by the Information Protection Officer on an ongoing basis. Staff should be made aware that this is being done. An IT system or automatic audit trail may need to be put in place to support this supervision.

CONCLUSION

For the first time, South Africans will have their constitutional right to the privacy of their PI enforced. POPIA will bring South Africa in line with international data protection laws and at the same time, will protect PI collected and processed by public and private organisations.

PI privacy presents a growing challenge and Axiomatic must adapt and comply with complex international laws on how they handle such information. POPIA requires Axiomatic to establish appropriate policies and procedures to protect the various forms of data that are part of their business operations.

It is almost impossible to anticipate all eventualities and possibilities but strict adherence to this Policy together with heightened awareness of all Axiomatic staff will ensure that the company not only complies with the relevant legislation but ultimately, safeguards the PI entrusted to it by Axiomatic employees.