POPI stands for the "Protection of Personal Information"

The POPI Act (hereinafter referred to as "the Act") was passed into law by Parliament in 2013 and was **officially enforced on 1 July 2020**. The Act gives effect to the constitutional right to privacy by safeguarding and regulating personal information held on servers or files and processed by responsible parties, (including but not limited to various players in the property industry), namely Estate Agents, Mortgage Originators, Banks, Insurers and Attorneys. Each role player has one year within which to ensure that their business practices are in line with the Act, failing which they will face serious consequences of their breach, whether it is intended or not.

The Act seeks to ensure that personal information relating to individuals and juristic entities, (hereinafter referred to as "data subjects"), is dealt with in a responsible way so as to avoid same becoming available to third parties who are not entitled thereto without their consent. We suggest to make sure that your Sale or Lease Agreement contains a clause whereby the data subjects consent to you collecting, storing and processing their personal information, (for example to Bank Consultants, Mortgage Originators), in a way that benefits them and also allows the sharing of such information between yourselves, the Conveyancers and originators. An example of such clause would be as follows:-

"The parties herein hereby consent, as required under the Protection of Personal Information Act No. 4 of 2013 ("POPI"), to the Agent, Conveyancer and Mortgage Originator (if applicable) gathering our personal information. The Estate Agency, its Agents and supporting staff will have access to our personal information which we have given to them for the express purpose of concluding a binding Sale Agreement and transfer of immovable property.

The parties further consent to the sharing of our information between the Estate Agency, Conveyancers and Mortgage Originator (if applicable) so that the provisions of the Financial Intelligence Centre Act may be complied with by the respective organisations."

There are eight "processing conditions" which are set out by the Act which must be followed when information is collected, stored, handed out, used or deleted; namely:-

1. Accountability:

All businesses and private persons need to be responsible, accountable and comply with the conditions as set out under the Act.

2. Processing limitation:

Agents must only request data subjects to supply them with the personal information needed in order to conclude a binding sale agreement (i.e being the original purpose for which the information was requested in the first place).

3. Purpose specification:

Personal information must be collected for a specific and lawful purpose related to, for example, the conclusion of a binding sale agreement, and data subjects must be aware of same. Estate Agencies may not retain information for longer than necessary, (being 5 years unless the Property Practitioner's Act comes into existence which may require 10 years), whereafter it must be deleted or destroyed depending on whether it is in digital form or a hard copy (deletion off data base and paper shredding).

4. Further processing limitation:

Remember that any further use and processing of information, (for example to Banks and Attorneys), must be in line with the original purpose of such information being collected and it's important to obtain a person's consent thereto.

5. Information quality:

Always ensure that personal information obtained from a person is accurate, not misleading and updated where necessary.

6. Openness:

Estate agencies must ensure that data subjects are aware why certain personal information is being collected, the name and address of the Agency, the right of access to and the right to rectify information collected.

7. Security safeguards:

Estate agencies must treat information supplied to them by data subjects with the highest degree of privacy and care. It is imperative to ensure that digital customer relations management systems adhere to the regulations set out under the Act so it is important to partner with a service provider who will ensure that personal information is identified, processed in line with the Act and that the required consent is obtained on databases. Don't leave data subjects personal information lying on a desk or stored on a laptop left visible in a car where it could be the target of a would-be-thief. Have your computers set up whereby they automatically go into "sleep mode" if you are away from your computer and not actively working thereon for a certain period of time. Make sure that passwords to computers are kept safe and secure. Make sure that safeguards are regularly updated in the event of new risks or flaws in previously implemented safeguards. If there happens to be a security breach, it's important that the Agency informs the Information Regulator and the data subject whose personal information has been compromised.

8. Data subject participation:

A data subject, (who has provided adequate proof of identity), and who has provided an Estate Agency with personal information may request such Agency to furnish them with confirmation that the Agency holds their information as well as the particulars of such information and details of third parties who have also had access to such information. A data subject may also request an Agency to destroy (after 5 years) or update personal information.

Marketing

Marketing is a critical aspect of every Estate Agents and Agencies tool-kit. The Act not only stipulates that permission is always required for the distribution of a data subjects' personal information but data subjects are also in control of outside information which they receive! The Act impacts the way in which Estate Agents can market homes. Estate Agencies and Agents are not allowed to send potential data subjects any direct marketing materials unless the data subject is already an existing client on their database, (however the data subject must have the option to unsubscribe should he or she wish to do so otherwise they will be in contravention of the Act), or if the potential client consents to receiving various marketing material.

A breach of the Act resulting in the unlawful sharing of information has far-reaching consequences, depending on the severity. A data subject can report a matter to the Information Regulator, (being a committee appointed in terms of the Act), and if after investigation the Regulator finds that an abuse or compromise of personal information has occurred it can result in the Information Regulator issuing a fine of up to a maximum amount of R10 million or imprisonment of up to 10 years.

Defences

Defences to the defaulting party are limited by the Act. The Defendant would need to prove that:-

1. The Regulator exempted them;
2. Compliance was not reasonably practical;
3. The Plaintiff consented or was at fault themselves; or
4. The breach was an act of God.

If you have any queries please contact Annabelle