Publication: Cover
Date: 01 Nov 2016
Page: 85

Be careful how you deal with client information

LOUIS VAN VUREN
CEO, Fiduciary Institute of Southern Africa (FISA)

Fiduciary practitioners will in future have to be very careful how they deal with the personal information of clients.

Although the confidential treatment of client information is almost synonymous with the fiduciary duty of executors and trustees, there are new requirements on their way regarding the proper safeguarding of client records.

The Protection of Personal Information Act, 4 of 2013, ("POPI") was signed into law by the president on 19 November 2013. However, only the parts of the act relating to establishing the office of the information regulator have become effective. The rest of the act will become effective on a date which is yet to be announced.

The rationale for the act is to manage the tension between the fundamental constitutional value of openness in section 1 of the Constitution, 1996, and the individual's right to privacy in section 14 of the Constitution.

Any processing of personal information of an individual, except for purely household or personal purposes, for journalism, art or literature, or for criminal prosecution or national security purposes, must be done by a responsible party in accordance with the requirements set out in the act.

Any fiduciary practitioner will be a responsible party and will have to comply with the act in all actions with regard to personal information of clients.

Personal information may only be processed with the consent of the person to whom it relates. Exceptions to this rule are if processing is required by law, if it is necessary to conclude a contract with such a person, if it protects a legitimate interest of the person to whom it relates, or if it is necessary to pursue a legitimate interest of the responsible party.

Personal information may only be collected for a specific, lawful purpose and may not be kept longer than necessary. The person to whom it relates must be informed of the purpose of processing and must be given adequate time to request the record before the information record is destroyed.

A trustee will be allowed to keep information about any party linked to the trust under the requirement in s17 of the Trust Property Control Act, 57 of 1988, because a requirement in law to keep information exempts the responsible party from the demand not to keep personal information beyond the expiry of its original purpose. If a code of conduct requires it, information may also be kept.

Given the extremely long time periods for which a client relationship may exist, a fiduciary practitioner will probably be entitled to claim that the continued maintenance of a client record is essential to protect the legitimate interests of both the practitioner and the client. This obviously makes the duty on the practitioner to be extremely careful about how the information is dealt with even more onerous.

The responsible party must also ensure that personal information is complete, accurate, not misleading and updated where necessary, keeping the purpose of processing the information in mind.

The client (or person to whom the information relates) must be informed of the purpose of the processing of information, where and how it will be kept, who the responsible party is, whether the supply of the information is mandatory (e.g. under a legal duty) or voluntary, what other parties will have access to the information, the right to object to processing of the information and the right to complain to the office of the information regulator.

In the absence of a duty to do so, the responsible party may not share personal information with any other party without the consent of the person it relates to. This writer's opinion has always been that this is just good manners. Sharing of client information in a group of companies for so-called "cross-sell" purposes without the client's express permission will therefore no longer be allowed. Selling a database will also no longer be legal.

A responsible party will also have to safeguard personal information against unlawful access or processing, as well as loss or unauthorised destruction of or damage to the information. This implies regular back-ups of electronic records, and regular risk assessments of virus protection and anti-hacking measures. The act requires risk assessments and regular updates to protect against new threats. Hard copy records will similarly have to be protected against theft, loss or damage.

The person to whom the information relates may request confirmation from a responsible party as to what data is held and for what purpose, who else has access to it, and request that a record be corrected. In doing so, the request process prescribed by the Promotion of Access to Information Act, 2 of 200, must be followed.