

The pros and cons of deed digitisation

In July, the Deeds Office officially entered the digital era when the Bloemfontein office registered its first property transfer with a digitally signed document, paving the way to a more efficient and streamlined process in an industry which is renowned for cumbersome reams of documentation



Arnold Maritz, Southern Suburbs co-principal for Lew Geffen Sotheby's International Realty, says: "When one considers that there are only 10 deeds offices country-wide, an innovation that facilitates the registration process is most welcome, and this change alone can speed up the lengthy sale process by a few days.

"This step is part of a broader transformation to be implemented under The Deeds Registries Amendment Bill, 2015 that also provides for an electronic deeds registration system, the electronic keeping of register and the electronic issuing of deeds for information and judicial purposes only."

Pen and ink

He adds that although the document submitted in Bloemfontein was a Power of Attorney, the Deeds Office has since ruled that this document as well as the Deed of Sale must still be hand-signed in pen before being lodged together with the other documents, so a significant amount of paperwork and facetime is still necessary.

"When a fully digital system that is safe, user-friendly and accessible is developed, it will change the way property sales are handled," says Lara Colananni, specialist conveyancing attorney from Guthrie Colananni Attorneys.

"However, at this stage it is still necessary to physically FICA individuals, companies and trusts, and not all documents can be signed electronically. Using trusted encryption techniques, like biometrics, will be far more efficient and less risky, if highly sophisticated electronic security and firewalls are out in place."

Given the spike in digital fraud in the real estate industry in recent years, many people are understandably

apprehensive and concerned that further digitisation will create new opportunities for brazen fraudsters.

Colananni says: “Innovation and change often increase risks because it is just a matter of time before an enterprising criminal finds a way to abuse the new system. Then, it comes right back to cops and robbers.

“The key factor is that when entering into digital contracts, you have no idea who is on the other side of an email address. Identity theft and digital editing make it possible to create false online identities and many of these fake profiles are so convincing that even astute parties may be duped.”

Staying protected while saving paper

So how does one protect oneself without staying in the dark ages, killing half a forest with each transaction

It is essential to sign documents through recognised and reputable encryption agencies that facilitate advanced electronic signatures. Advanced electronic signatures aren't signatures made by hand, scanned and pasted onto a document – they are encrypted, using a public and private key system, so that if information is intercepted in cyberspace it cannot be read.

“In other words, it will read like gibberish until the party receiving it unlocks it, or decodes it with a matching key,” says Colananni.

“Advanced e-signatures also serve to confirm the identity of the person on the other side of the digital correspondence, because encryption agencies verify identity before granting keys.

“Biometrics, like face recognition or finger prints also unlock encrypted information. A perfect example is Whatsapp messages, which are encrypted until the recipient of the message unlocks their phone using a code or a thumb print. However, there is a risk that a cybercriminal could find a way to copy the key that decodes the information.”

Colananni believes that there will definitely be more pros than cons once all legal procedures become digitised, because it will make legal services cheaper, faster and more accessible to the public, however, the cons will not be of minor significance, relating to identity theft, fraud and monetary theft.

“While digitisation is safer theoretically, a recurring problem with cybercrime is that in many instances there is no trace of the perpetrator after the fact. In the event that someone's online identity is stolen, it will be possible for the thief to sell their property and disappear with the proceeds of sale.”

Maritz concludes: “As the industry continues to digitise, it will become increasingly critical for buyers and sellers to ensure that they appoint accredited, experienced and knowledgeable professionals. The diminishing human connection will become all the more important in circumnavigating cyber fraud which will be adapting as quickly as technology advances.”