No *shred* of evidence

What steps can organisations take to destroy personal information?

Many organisations have begun to consider how best to comply with the requirements of the Protection of Personal Information (POPI) Act in terms of erasure or destruction of personal information (PI).

This includes the ability to erase, delete or destroy PI once there is no justifiable reason (based on legislative compliance or business need) to retain the PI any longer. Included in this is the need to comply with requests from Data Subjects to have their PI destroyed or deleted (Chapter 2, section 5 of the POPI Act). The POPI Act says that deletion or destruction must be done "in a manner that prevents its reconstruction in an intelligible form" (Condition 3, section 14 of the POPI Act). So now we know what the POPI Act requires, what steps can organisations take?

A useful first step is to identify the different data media which need to be destroyed. For this exercise the DIN-66399 standard (www.din-63399.com) can prove helpful to identify seven categories of media: information in original size, for example paper, films or printing plates; in miniaturised form, for example microfilms; on optical data carriers, for example CDs/DVDs; on magnetic data carriers, for example ID-cards or diskettes; on hard drives with magnetic data carriers; and on electronic data carriers, for example flash drives or chip cards.

In addition DIN-66399 provides for seven security levels of destruction which vary according to the particle size which results from the destruction process: Security Levels P1 to P2 rely on traditional ribbon or strip cut and can result in strips widths from under 12mm (P1) to under 6mm (P2). Security levels P3 to P7 reduce the permitted particle size to from under 320mm^2 to under 5mm^2, which offers the highest level of security.

When proper consideration is given to applying these standards, simply attempting to tear up or manually shred the various media types becomes unworkable. Even worse, incinerating the media may be dangerous and environmentally unacceptable.

DIN-66399 is also helpful when considering the sensitivity of the different types of data to be destroyed. Classification Level 1 deals with normal sensitivity of internal data which would have limited negative effects should there be unauthorised disclosure or loss. Importantly, DIN-63399 excludes Personal Data (called PI in the POPI Act) in Classification Level 1 being protected by Security Level 1 or 2 methods – in other words, a traditional ribbon or strip cut shredding process is inadequate for POPI Act needs. Classification Level 2 deals with higher sensitivity information, where "unauthorised disclosure would have serious effects" and "may lead to violations of laws or contractual obligations". At Classification Level 2 protection of personal data will meet "stringent requirements". Finally, Classification Level 3 addresses confidential and secret information where unauthorised disclosure would have "serious existence-threatening effects" and protection of personal data will be absolutely guaranteed. Only Security Levels 4 to 7 should be used for the highest Classification Level 3 information destruction.

One additional consideration is whether the destruction or deletion complies with any other constraints which exist, such as a Records Management Policy (RMP) which the organisation may have in place. Part of an RMP, or a standalone policy or procedure, could contain practical advice on destruction aimed at staff who need to decide what to destroy, when.

The choice then exists as to whether to shred on site or to use a service provider. Here's what some of the leading industry players in South Africa had to say:

"Although standards such as EN15713 for remote shredding services exist in Europe, there has been little in the way of adoption in South Africa. This means that most paper shredding will continue to take place on-premise, using the type of advanced shredding devices we are well known for," says Bill Bayley, MD of Rexel Office Products.

"When it comes to electronic deletion, our customers understand why they need to consider effective electronic destruction of their data by not just using the Recycle Bin while leaving the device capable of re-use (sanitisation) or complete electronic (degaussing) or physical destruction (shredding) of their digital storage devices, and that's something very few organisations are equipped to do on their own," says Wale Area, chief executive and founder of Xperien.

In summary, the POPI Act requirements place obligations on organisations to plan and implement effective PI destruction, and most organisations will likely adopt a hybrid approach, combining the cost-effectiveness of on-premise shredding with the use of specialised digital shredding services for their advanced needs.

So the question remains: what will you do? ■

ACKNOWLEDGEMENT
DR PETER TOBIN
@SAPOPITALK