



## Areas to Note When Disposing Personal Data

***Imagine opening a gift hamper and finding that the packing material had bits of order form with the personal data of other customers on it? Or while queuing to board a plane, you pass by a rubbish bin and see a partially printed passenger name list comprising personal data. One may think such situations could never happen. But they did.***

Mid last year, the Personal Data Protection Commission (PDPC) issued directions to a data intermediary of an airline company and a warning to a gift company for failing to put in place reasonable security arrangements (which includes ensuring proper handling of personal data and the review of personal data protection practices) to prevent the accidental disclosure of personal data.

These two cases highlight one aspect of the care of personal data that often received insufficient attention among some organisations, i.e. the proper disposal of personal data.

The Protection Obligation (Section 24) of the Personal Data Protection Act (PDPA) requires an organisation to make reasonable security arrangements to protect personal data in its possession or under its control in order to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks.

Some organisations do not realise that their responsibility over the protection of personal data does not end with the information simply being discarded in the trash bin, regardless of whether it is in physical or electronic form.

Improper and incomplete disposals can lead to personal data breaches.

Sharing his company's approach to personal data protection, Mr Michael Lim, Legal & Compliance Manager of LG Electronics Singapore, said one essential component of its data protection strategy is to examine the life cycle of personal data from the point of collection to its destruction.

"This is to ensure that there are proper procedures for the protection of the personal data at each point of the life cycle," said Mr Lim. "Proper disposal of personal data is therefore an important element in our overall protection strategy."

## Common Mistakes in the Disposal of Personal Data

Mr Duncan Brown, General Manager of Shred-it Singapore, which provides onsite and offsite information destruction services, said that paper is perceived by many organisations as valueless once it is no longer needed. Little care is then placed on the disposal process, making unauthorised access to the information easy, both inside and outside of the organisation.

A particular area that organisations tend to overlook or be complacent about is the cleaner's access to waste paper. Mr Brown observed that there had been numerous occasions where waste paper ends up being sold to a karung guni (a rag-and-bone man who buys and sells used-items such as electrical appliances and unwanted papers), and this was where unauthorised access to personal data occurred.

Echoing this point, Mr Emmanuel Tay, Commercial Analyst at Sembcorp Tay Paper Recycling, said this is akin to "trading your 'million-dollar' information away for a few dollars".

"This method provides no means of auditability. That document could change hands a few times before it is destroyed, increasing the risk of the document landing into the wrong hands."



"This method provides no means of auditability. That document could change hands a few times before it is destroyed, increasing the risk of the document landing into the wrong hands."

**- Mr Emmanuel Tay**  
Commercial Analyst  
Sembcorp Tay Paper Recycling Pte Ltd

In an effort to be environmentally friendly, organisations often introduce potential data breach risks by having secure disposal bins situated next to recycling bins. As Mr Brown observed, "what we often see is that well-

meaning employees place documents that contain personal data of a sensitive nature in the recycle bins instead of in the secure disposal bin." To counter this, Shred-it recommends that organisations adopt a "Shred-All" policy which eliminates the need for employees to decide what is confidential and what is not.



"What we often see is that well-meaning employees place documents that contain personal data of a sensitive nature in the recycle bins instead of in the secure disposal bin."

**- Mr Duncan Brown**  
General Manager  
Shred-it Singapore Pte Ltd

Another area that is often overlooked is how easy it is for data to be transferred from one medium to another. "A piece of paper, or a pile of documents, can easily be scanned and find their way into the 'cyber' realm. Similarly, and vice versa, electronic documents can easily be printed out," he added.

For personal data stored in electronic or optical storage media (hard disks, solid state drives, flash drives, CDs, DVDs, etc.), one common mistake is to assume that the "delete", "clear recycle bin" and "format" commands used in standard operating systems tantamount to erasure of the data. Most operating systems do not fully delete the actual file in the storage media. These commands simply delink the "deleted" file from the user's view; the data still resides in the system until it is overwritten by new files. Commonly available software can recover these "deleted" files.

Additionally, the practice of selling outdated electronic assets to third parties, returning them to vendors or throwing them away without the complete erasure of personal data could lead to recovery and unauthorised disclosure of such data therein, which is in breach of the protection obligations of the PDPA.





### **Disposal of Personal Data on Physical Media**

The appropriate disposal process chosen by organisations should transform or destroy personal data in a way where it can no longer be used to identify or relate to a person.

For personal data stored on paper, proper disposal or destruction usually involves processes such as shredding, incineration or pulping.

Depending on the category of information stored on the document, different shredder specifications may be required to properly shred the paper. For example, cross-cutting capabilities or confetti shredders make it much more difficult for a third party to reassemble individual pieces of paper into the original documents, compared to the use of a straight-cut shredder.

With incineration, paper is reduced to ashes. Pulping involves the mixing of paper with water and chemicals to break down the paper fibres before recycling them.

At LG Electronics Singapore, there is a standing policy that all paper documents that contain personal data or confidential information are not to be disposed of in waste paper baskets, but in specific secure bins designated for such disposal, said Mr Lim.

The secure bins are locked, and no one can retrieve the documents except for the legal and compliance department which serves as the company's Data Protection Office and holds the keys to the bins.

Bi-weekly, the company's service provider will clear the bins. The documents are brought to the service provider's truck which is equipped with a paper shredder, and LG's legal manager will ensure that the documents are shredded on the spot.

For more information, please refer to [PDPC's Guide to Disposal of Personal Data on Physical Medium](#).

### **Ensuring Proper Destruction of Electronic Personal Data**

When data is stored in electronic form, organisations have to take steps to ensure that it is securely deleted, erased or destroyed before the storage media is redeployed, exchanged or disposed of.

Total deletion or disposal of data in electronic (re-writable) medium is commonly referred to as "sanitisation".

Some common methods of disposal include

software solutions that securely overwrite data, degaussing, and destruction.

Degaussing refers to the removal of magnetic fields using a machine that destroys any magnetically recorded data. Mr Tay warned that while data may be erased through the degaussing process, it can still be restored using technology when not done properly. Destruction methods such as shredding, crushing or incineration, on the other hand, ensure complete destruction of the electronic medium, so there is no risk of re-use or the data being restored.

For LG Electronics Singapore, Mr Lim shared that the organisation's policy for the disposal or deletion of personal data contained in electronic media is that it has to be done permanently, i.e. in a way that the personal data cannot be recovered.

"When an equipment, for example laptop or server, is to be discarded, the data storage media will be removed and discarded separately. Where the data storage media is to be discarded, it will be destroyed physically," said Mr Lim.

For more information, please refer to [PDPC's Guide to Securing Personal Data in Electronic Medium](#).



"When an equipment, for example laptop or server, is to be discarded, the data storage media will be removed and discarded separately. Where the data storage media is to be discarded, it will be destroyed physically"

**- Mr Michael Lim**  
Legal & Compliance Manager  
LG Electronics Singapore

## Managing Third-Party Service Providers

Disposal of personal data can be carried out in-house by the organisation itself or by a third-party service provider.

It is important to remember that the organisation that outsources its process to a third party is still accountable for the personal data. The organisation must ensure that the external processing is still in compliance with the Protection Obligation of the PDPA.

The organisation that outsources its processes should ensure that its contracts with third-party service providers contain the necessary terms and conditions to require that service providers comply with the PDPA. It will also need to understand how these service providers would dispose the media as well as the downstream supply chain arrangements that are involved.

Mr Lim reiterated that for LG Electronics Singapore, all its vendors need to sign a special agreement which requires that the vendor disposes personal data in a proper manner.

## Conclusion

Data disposal should not be taken lightly, especially if it comprises personal data.

The protection of personal data does not end with it being discarded in a physical or electronic trash bin. The disposal process needs to be well managed and controlled so that the risk of recovery and accidental disclosure is reduced.