

How Can Your Organisation Dispose Of Personal Data?

Organisations today collect, use and disclose personal data about individuals for various reasons and through multiple avenues. Your organisation may hold a wealth of personal data relating to customers or employees for business or legal purposes.

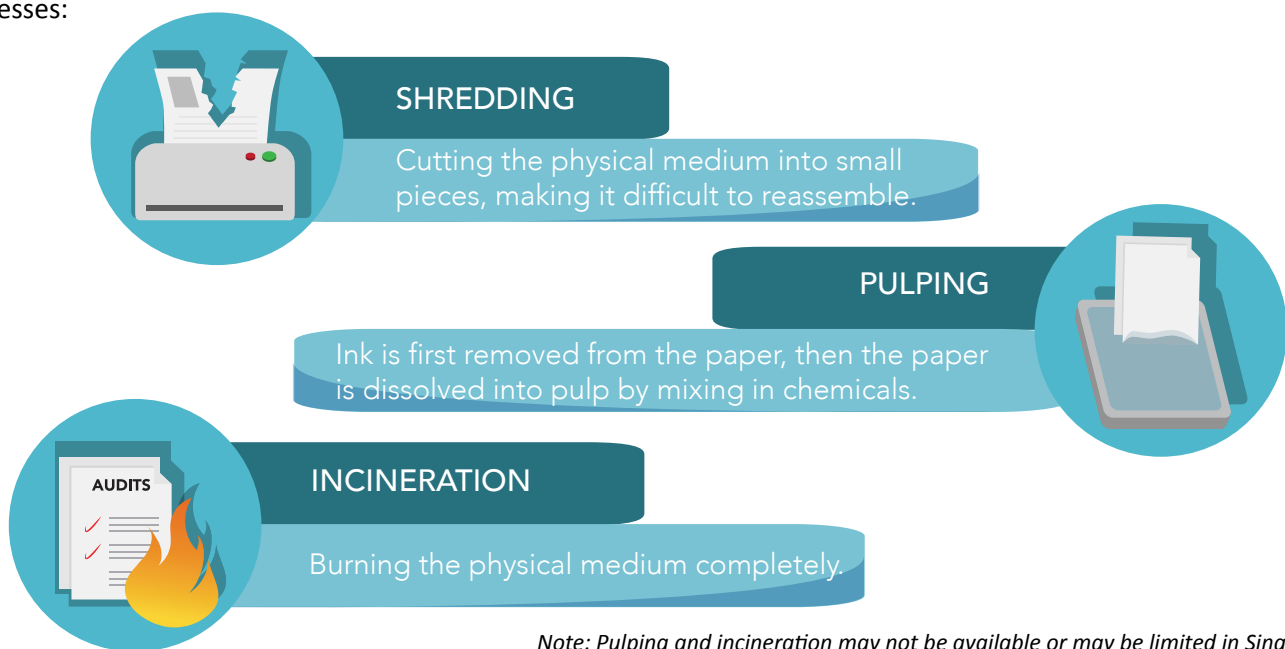
Keeping personal data longer than necessary, however, leads to more effort in tracking such records, and can also increase the resources and cost to protect it.

Consider setting clear retention periods for the various types of personal data that your organisation holds. Review the personal data regularly and dispose of anything that is no longer needed.

Physical Destruction

The common practice of destroying physical media is by tearing them into halves (e.g. letters, documents and cards in paper form) or breaking them into two (e.g. read-only CDs and DVDs). They are then disposed into a bin. However this does not destroy the personal data completely. The pieces can be reassembled, thereby placing the personal data on it at risk.

Organisations should consider disposing physical media in a secure manner through one or more of the following processes:



Note: Pulping and incineration may not be available or may be limited in Singapore.

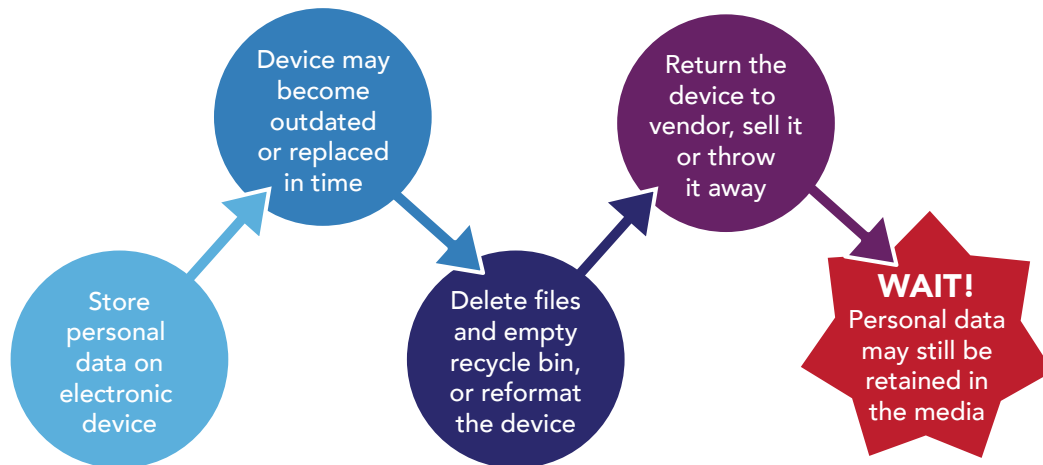
Adopting Good Practices in the Office

- When in doubt whether the physical media contain personal data, shred them;
- Do not leave physical media unattended in common areas if they contain personal data, even if they are meant to be discarded; and
- Maintain and clear the shredder regularly. Otherwise, employees may be tempted to opt for less secure methods of disposal if the shredder cannot be used.

For more information, please refer to the Guide to Disposal of Personal Data on Physical Medium at www.pdpc.gov.sg.

Electronic Destruction

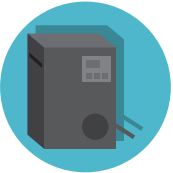
It is a common assumption that files are completely destroyed after they are deleted and the recycle bin is cleared. However, the computer simply hides them from view and there are certain software that can recover the “deleted” files.



With at least one of the following steps, your organisation will be able to permanently destroy or remove electronic data:



- Use dedicated software that can overwrite selected files or the entire storage drive.



- Use specialised hardware appliances that cater for the destruction (e.g. a degausser machine produces a strong electromagnetic field that can destroy magnetically recorded data).



- Physically destroy the storage device by crushing, drilling or shredding it.

Alternatively, your organisation may anonymise the personal data and keep it for further uses. This is a form of disposing personal data. However, be mindful that anonymised data, when combined with other data, may re-identify an individual. Organisations considering this option should take steps to address re-identification risks.

For more information, please refer to the Guide to Securing Personal Data in Electronic Medium and the Anonymisation chapter in the Advisory Guidelines on the PDPA for Selected Topics at www.pdpc.gov.sg.

COPYRIGHT 2016 – Personal Data Protection Commission Singapore and Info-communications Development Authority of Singapore

This publication gives a general introduction on the disposal of personal data in physical and electronic media. The contents herein are not intended to be an authoritative statement of the law or a substitute for legal advice. The Personal Data Protection Commission (PDPC), the Info-communications Development Authority of Singapore (IDA) and their respective members, officers and employees shall not be responsible for any inaccuracy, error or omission in this publication or liable for any damage or loss of any kind as a result of any use of or reliance on this publication.

The contents of this publication are protected by copyright, trademark or other forms of proprietary rights and may not be reproduced, republished or transmitted in any form or by any means, in whole or in part, without written permission.