Anonymising personal data means removing from the personal data any information from which an individual may be identified by anyone reading the record. Anonymisation also means that the data user is not in a position to establish the identity of any individual with its other existing or future information on the individual. Most importantly, data user should commit, by clear policy, that it does not and will not attempt to re-identify any individuals from anonymised data or to use the information or any individuals even if re-identification is possible.

Simply removing names, addresses or other such obvious identifiers (such as biometric data) may not be sufficient to make the data fully anonymous. When data contains complex or unique descriptions of individuals, it may be practicable for others to identify them even if the data does not contain any obvious identifiers. For example, if the data is related to a small group of people, such as a certain class of students, individuals may be reasonably ascertained if certain indirect identifiers, such as their area of residence, years attended, academic results on specific subjects/areas, are kept.

Furthermore, with the advancement of information technology, it may be possible for the data user or any third parties to ascertain or reasonably ascertain the identities of individuals using other publicly available information. To prevent this, data users must consider carefully whether or not to release the anonymised data to third-parties or the public.

Data users must realise that using anonymisation instead of erasure entails the risk that individuals may be re-identified from the data in the future. In this era of Big Data, there has been growing concern whether in the case of very large databases it will still be possible to genuinely and effectively anonymise individuals. Data users must take all practicable steps to erase personal data held when the data is no longer required for the purpose for which it was used.

Furthermore, when disposing storage holding personal, data users must take practicable steps to ensure that the personal data is erased and cannot be retrieved as a result of the disposal.

This guidance note provides advice as to when personal data should be erased, as well as how personal data may be permanently erased by means of digital deletion and/ or physical destruction.

This guidance note also introduces the alternative of anonymisation, which de-identifies personal data to the extent that it is no longer practicable to identify an individual directly or indirectly, in which case the data would not be considered as personal data under the Personal Data (Privacy) Ordinance ("the Ordinance").

Legal Requirements related to Personal Data Erasure

Section 26 of the Ordinance provides that a data user must take all practicable steps to erase personal data held when the data is no longer required for the purpose (including any directly related purpose) for which it was used, unless any such measure is prohibited under any law or is in the public interest not to have the data erased.

Data users engaged in the collection, holding, processing or use of personal data must carefully consider how to ensure such personal data when it is no longer required for the purpose for which it was used.

Furthermore, when disposing storage holding personal, data users must take practicable steps to ensure that the personal data is erased and cannot be retrieved as a result of the disposal.

This guidance note provides advice as to when personal data should be erased, as well as how personal data may be permanently erased by means of digital deletion and/ or physical destruction.

This guidance note also introduces the alternative of anonymisation, which de-identifies personal data to the extent that it is no longer practicable to identify an individual directly or indirectly, in which case the data would not be considered as personal data under the Personal Data (Privacy) Ordinance ("the Ordinance").
In order to comply with section 26 and DPP2(2), data users must have a personal data retention policy that sets out specific management practices on how each type of records, digital or physical, is to be identified for erasure.

Similarly, in the case of digital records, an appropriate method must be deployed to permanently delete data from each specific type of electronic storage device. Simple file deletion or reformatting of hard drives and USB memory devices are not reliable methods of deleting data, as can be fully recovered by commonly available third-party software. Instead, it is recommended that dedicated software, such as those conforming to industry standards (e.g. US Department of Defence standards, the DoD 5220.22-M standard), be used to permanently delete data on various types of storage devices, such as hard drives or USB memory devices. Such software may take a long time (in terms of cost and in terms of elapsed time) to perform. In many cases, it results in a complete and secure record. For records residing in servers, an appropriate method should be chosen to delete the data, bearing in mind any facilities within the server that can be used to recover records or files, such as an "undelete" command that can be used to recover previously erased files on a server.

Physical destruction remains an effective means of deleting electronic records typically depending on the whole storage medium (repercussion of media destruction is much easier to control than physical destruction of digital records). This is particularly appropriate in cases where the records can no longer be accessed or reconstructed (e.g. burn paper, break hard disk or USB memory devices that appear to be broken). While physical destruction methods will often render the media unusable, they may be considered as the last resort by data users, especially when information stored in it has different retention requirements; and (iv) the consequence of any non-compliance with the relevant requirements under the Ordinance. At the very least, the data user should contract the requirements for erasure on (i) the security requirements relating to the transportation and handling of the personal data; (ii) the extent that personal data would be disclosed without going through a secure process; (iii) the mechanism to ensure/confirm that all personal data has been removed.

Recycling

Recycling is the risk of data breach associated with recycling. It is important that personal devices are removed in a way that ensures their data is rendered unreadable or inoperable. This is particularly important when dealing with employees who work remotely or are frequently away from the office premises or off-site, which would involve transporting personal devices for disposal or recycling.

An holistic approach to the management of personal data is required for the management of data destruction. This involves the development of an integrated organisational-wide policies, guidelines and/or procedures. Without a top-down approach, records or devices holding personal data may be kept longer than necessary or discarded untrusted.

A holistic approach to the management of personal data is required for the management of data destruction. This involves the development of an integrated organisational-wide policies, guidelines and/or procedures. Without a top-down approach, records or devices holding personal data may be kept longer than necessary or discarded untrusted.

Destruction vs Anonymisation

Total erasure is not necessarily the only option for handling personal data no longer required for the performance of the organisation's core business activities. Where possible, data users should consider anonymising personal data where it is feasible to do so, for example, where personal data has no meaningful identifiers or where it can be matched only with personal identifiers that are not necessary or desirable.
In order to comply with section 26 and DPP(2), data users should have a personal data erasure policy that sets out specific management practices on how each type of record, digital or physical, is to be identified for erasure.

A decision must be made as to whether the shredded wastes should be specially handled or can be thrown away with normal office waste. Another issue which needs to be addressed is how to ensure that the destruction is carried out in the organisation’s premises or off-site. In order to comply with the requirement to protect personal data outside the data user’s premises.

Similarly, in the case of digital records, an appropriate method must be deployed to permanently delete data from each specific type of electronic storage device. Simple file deletion or reformatting of hard drives and USB memory devices are not reliable methods of deletion, as data can be fully recovered by commercially available third-party software.

It is clear from section 26, DPP(2) and DPP(3) that when personal data is no longer required for the purpose for which it is or is to be used by the data user, it is required for the management of data destruction.

It is clear that from section 26, DPP(2) and DPP(3) that when personal data is no longer required for the purpose for which it is or is to be used by the data user, it is required for the management of data destruction.

It is clear that from section 26, DPP(2) and DPP(3) that when personal data is no longer required for the purpose for which it is or is to be used by the data user, it is required for the management of data destruction.

It is clear that from section 26, DPP(2) and DPP(3) that when personal data is no longer required for the purpose for which it is or is to be used by the data user, it is required for the management of data destruction.

It is clear that from section 26, DPP(2) and DPP(3) that when personal data is no longer required for the purpose for which it is or is to be used by the data user, it is required for the management of data destruction.

It is clear that from section 26, DPP(2) and DPP(3) that when personal data is no longer required for the purpose for which it is or is to be used by the data user, it is required for the management of data destruction.
When personal data is no longer required for the purpose for which it is held by the data user, it is the responsibility of the data user to erase the data or to prevent it from being kept later than is necessary. Although DPCC concerns primarily the security of personal data, it also applies to the secure destruction of personal data or its copies held in paper forms or in storage devices. For examples, the destruction of paper records or photocopies which contain personal data, or the handling of obsolete information technology storage equipment for disposal or recovery.

A Holistic Approach

Expiry of retention period and disposal of records/stores are not necessarily the only situations in which data erasure is concerned about. Other less obvious situations may include shutiling apparently any other cloud service, or service provider (such as if specialised equipment is involved), must conduct regularly to raise awareness and make sure that all employees are playing their part effectively.

Retention and Erasure Policies

A decision must be made as to whether the shredded wastes should be specially handled or can be thrown away with normal office waste. Another issue which needs to be considered is whether there should be destruction by a contractor, as this is often the only way the personal data must be accounted for in the erasure exercise. This includes all photocopies, backup copies of all records, and the destruction of old computer equipment.

Recovery of data from storage devices. This is particularly appropriate where the contents of data, such as smartphones (including their memory cards), USB memory devices and mobiles devices, and any other cloud service, or service provider (such as if specialised equipment is involved), must conduct regularly to raise awareness and make sure that all employees are playing their part effectively.

Further more, both DPP2(1) and DPP2(2) require any data user engaging a service provider to process personal data to adopt contractual or other means to ensure that the service provider complies with the relevant requirements under the Ordinance. At the same time, data users must, when entering into the contract for the requirements for erasure on (i) the security requirements relating to the transportation and handling of the personal data, (ii) the erasure standard and service level; (iii) the mechanism to ensure/control that all personal data is erased according to the agreed requirements; and (iv) the consequent of non-compliance with the contract terms. For more information on the contract requirements, please refer to Information Leaflet 2 - Outsourcing the Processing of Personal Data to Data Processors published by the Commissioner.

Employee Awareness

This is an era of information technology, data users often allows their employees to access and download large amounts of personal data held by the data user. It is therefore very important to ensure that employers are aware of and adhere to the retention and erasure policies of an organisation. Sufficient training must be conducted regularly to raise awareness and make sure that all employees are playing their part effectively.

Destruction versus Annonymisation

Total erasure is not necessarily the only option for handling personal data no longer required for the purposes for which it was held. Data users may wish to retain part of the data for various reasons, such as for research and/or statistical purposes. If the personal data is in an anonymised form (or anyone else) will not be able to directly or indirectly identify an individual concerned, the data is not considered to be personal data under the Ordinance.
Anonymising personal data means removing from the personal data any information from which an individual may be identified by anyone reading the record. Anonymisation also means that the data user is not in a position to establish the identity of any individual with its other existing or future information on the individual. Most importantly, data user should commit, by clear policy, that it does not and will not attempt to re-identify any individuals from anonymised data or to use the information or any individuals even if re-identification is possible.

Simply removing names, addresses or other such obvious identifiers (such as biometric data) may not be sufficient to make the data fully anonymous. When data contains complex or unique descriptions of individuals, it may be practicable for others to identify them even if the data does not contain any obvious identifiers. For example, if the data is related to a small group of people, such as a certain class of students, individuals may be reasonably ascertained if certain indirect identifiers, such as their area of residence, years attended, academic results on specific subjects/areas, are kept.

Furthermore, with the advancement of information technology, it may be possible for the data user or any third parties to ascertain or reasonably ascertain the identity of individuals using other publicly available information. To prevent this, data users must consider carefully whether or not to release the anonymised data to third-parties or the public.

Data users must realise that using anonymisation instead of erasure entails the risk that individuals may be re-identified from the data in the future. In this era of Big Data, there has been growing concern whether in the case of very large databases it will still be possible to genuinely and effectively anonymise individuals. Data users must make sure that the benefits of keeping anonymised data outweigh the potential risk that such data may be used to re-identify individuals, and that re-identification, which de-identifies personal data to the extent that it is no longer practicable to identify an individual directly or indirectly, in which case the data should be erased, as well as how personal data may be permanently erased by means of digital deletion and/or physical destruction.

This guidance note provides advice as to when personal data should be erased, and as to how personal data may be re-identified from the data in the future. In this era of Big Data, there has been growing concern whether in the case of very large databases it will still be possible to genuinely and effectively anonymise individuals. Data users must make sure that the benefits of keeping anonymised data outweigh the potential risk that such data may be used to re-identify individuals, and that re-identification, which de-identifies personal data to the extent that it is no longer practicable to identify an individual directly or indirectly, in which case the data should be erased, as well as how personal data may be permanently erased by means of digital deletion and/or physical destruction.

This guidance note introduces the alternative of anonymisation, which de-identifies personal data to the extent that it is no longer practicable to identify an individual directly or indirectly, in which case the data would not be considered as personal data under the Personal Data (Privacy) Ordinance ("the Ordinance").

Legal Requirements related to Personal Data Erasure

Section 26 of the Ordinance provides that a data user must take all practicable steps to ensure personal data held when the data is no longer required for the purpose (including any directly related purpose) for which it was used to be erased, unless such an erasure is prohibited under any law or in the public interest not to have the data erased.

Data Protection Principle ("DPP") 2(2) in Schedule 1 to the Ordinance requires data users to take all practicable steps to ensure that personal data is not kept longer than is necessary for the fulfilment of the purpose (including any directly related purpose) for which the data is or is to be used.

Furthermore, when disposing storage holding personal data, data users must take practicable steps to ensure that the personal data is erased and cannot be retrieved as a result of the disposal.

This guidance note provides advice as to when personal data should be erased, as well as how personal data may be permanently erased by means of digital deletion and/or physical destruction.

This guidance note provides advice as to when personal data should be erased, as well as how personal data may be permanently erased by means of digital deletion and/or physical destruction.

Copyrights

The information provided in this guidance is for general reference only. It does not provide an exhaustive guide to the application of the Personal Data (Privacy) Ordinance. For a complete and definitive statement of law, direct reference should be made to the Ordinance itself. The Commissioner makes no express or implied warranties of accuracy or fitness for a particular purpose or use with respect to the above information. The above suggestions will not affect the functions and powers conferred upon the Commissioner under the Ordinance.

Disclaimer

The information provided in this guidance is for general reference only. It does not provide an exhaustive guide to the application of the Personal Data (Privacy) Ordinance. For a complete and definitive statement of law, direct reference should be made to the Ordinance itself. The Commissioner makes no express or implied warranties of accuracy or fitness for a particular purpose or use with respect to the above information. The above suggestions will not affect the functions and powers conferred upon the Commissioner under the Ordinance.

Guidance on Personal Data Erasure and Anonymisation

Introduction

Data users engaged in the collection, holding, processing or use of personal data must consider how to erase such personal data when it is no longer required for the purpose for which it was used.

Furthermore, when disposing storage holding personal data, data users must take practicable steps to ensure the personal data is erased and cannot be retrieved as a result of the disposal.

This guidance note provides advice as to when personal data should be erased, as well as how personal data may be permanently erased by means of digital deletion and/or physical destruction.

This guidance note introduces the alternative of anonymisation, which de-identifies personal data to the extent that it is no longer practicable to identify an individual directly or indirectly, in which case the data would not be considered as personal data under the Personal Data (Privacy) Ordinance ("the Ordinance").

Legal Requirements related to Personal Data Erasure

Section 26 of the Ordinance provides that a data user must take all practicable steps to ensure personal data held when the data is no longer required for the purpose (including any directly related purpose) for which it was used, unless any such erasure is prohibited under any law or in the public interest not to have the data erased.
Guidance on Personal Data Erasure and Anonymisation

Introduction

Data users engaged in the collection, holding, processing or use of personal data must carefully consider how to erase such personal data when it is no longer required for the purpose for which it was used.

Furthermore, when disposing storage holding personal, data users must take practicable steps to ensure that the personal data is erased and cannot be retrieved as a result of the disposal.

This guidance note provides advice as to when personal data should be erased, as well as how personal data may be permanently erased by means of digital deletion and/or physical destruction.

This guidance note also introduces the alternative of anonymisation, which de-identifies personal data to make the data fully anonymous. When data contains identifiers (such as biometric data) may not be sufficient to make the data fully anonymous. When data contains complex or unique descriptions of individuals, it may be practicable for others to identify them even if the data does not contain any obvious identifiers. For example, if the data is related to a small group of people, such as a certain class of students, individuals may be reasonably ascertained if certain indirect identifiers, such as their age, residence, years attended, academic results on specific subjects/areas, are kept.

Furthermore, with the advancement of information technology, it may be possible for the data user or any third parties to ascertain or reasonably ascertain the identities of individuals using other publicly available information. To prevent this, data users must consider carefully whether or not to release the anonymised data to third-parties or the public.

Data users must realise that using anonymisation instead of erasure entails the risk that individuals may be re-identified from the data in the future. In this era of Big Data, there has been growing concerns whether in the case of very large databases it will still be possible to genuinely and effectively anonymise individuals. Data users must make sure that the benefits of keeping anonymised data outweigh the potential risk that personal data may be used to re-identify individuals, and that the impact such re-identification would have on the individuals. For this reason, data users must review regularly whether anonymised data can be re-identified and take appropriate action to protect personal data.

Legal Requirements related to Personal Data Erasure

Section 26 of the Ordinance provides that a data user must take all practicable steps to erase personal data held when the data is no longer required for the purpose (including any directly related purpose) for which it was used, unless any such erasure is prohibited under any law or it is in the public interest not to have the data erased.

PPP2(3) provides that if a data user engages a data processor, whether within or outside Hong Kong, to process personal data on the data user’s behalf, the data user must adopt contractual or other means to prevent any personal data transferred to the data processor from being kept longer than is necessary for processing of the data.

PPP4(1) requires a data user to take all practicable steps to ensure that personal data held by it is protected against unauthorized or accidental access, processing, erasure, loss, or use, including the consideration of:

(a) the kind of data and the harm that could result if any of those incidents should occur;
(b) the physical location where the data is stored;
(c) any security measures in place (whether by automated means or otherwise) into any equipment in which the data is stored;
(d) any measures taken for ensuring the integrity, prudence and competence of persons having access to the data; and
(e) any measures taken for ensuring the secure transmission of the data.

Data Protection Principle (“DPP”) Section 1 to and the Ordinance requires data users to take all practicable steps to ensure that personal data is not kept longer than is necessary for the fulfilment of the purpose (including any directly related purpose) for which the data is used or is to be used.

Furthermore, when disposing storage holding personal, data users must take practicable steps to ensure that the personal data is erased and cannot be retrieved as a result of the disposal.

This guidance note provides advice as to when personal data should be erased, as well as how personal data may be permanently erased by means of digital deletion and/or physical destruction.

This guidance note also introduces the alternative of anonymisation, which de-identifies personal data to make the data fully anonymous. When data contains identifiers (such as biometric data) may not be sufficient to make the data fully anonymous. When data contains complex or unique descriptions of individuals, it may be practicable for others to identify them even if the data does not contain any obvious identifiers. For example, if the data is related to a small group of people, such as a certain class of students, individuals may be reasonably ascertained if certain indirect identifiers, such as their age, residence, years attended, academic results on specific subjects/areas, are kept.

Furthermore, with the advancement of information technology, it may be possible for the data user or any third parties to ascertain or reasonably ascertain the identities of individuals using other publicly available information. To prevent this, data users must consider carefully whether or not to release the anonymised data to third-parties or the public.

Data users must realise that using anonymisation instead of erasure entails the risk that individuals may be re-identified from the data in the future. In this era of Big Data, there has been growing concerns whether in the case of very large databases it will still be possible to genuinely and effectively anonymise individuals. Data users must make sure that the benefits of keeping anonymised data outweigh the potential risk that personal data may be used to re-identify individuals, and that the impact such re-identification would have on the individuals. For this reason, data users must review regularly whether anonymised data can be re-identified and take appropriate action to protect personal data.

Legal Requirements related to Personal Data Erasure

Section 26 of the Ordinance provides that a data user must take all practicable steps to erase personal data held when the data is no longer required for the purpose (including any directly related purpose) for which it was used, unless any such erasure is prohibited under any law or it is in the public interest not to have the data erased.

Data Protection Principle (“DPP”) Section 1 to and the Ordinance requires data users to take all practicable steps to ensure that personal data is not kept longer than is necessary for the fulfilment of the purpose (including any directly related purpose) for which the data is used or is to be used.

Furthermore, when disposing storage holding personal, data users must take practicable steps to ensure that the personal data is erased and cannot be retrieved as a result of the disposal.

This guidance note provides advice as to when personal data should be erased, as well as how personal data may be permanently erased by means of digital deletion and/or physical destruction.

This guidance note also introduces the alternative of anonymisation, which de-identifies personal data to make the data fully anonymous. When data contains identifiers (such as biometric data) may not be sufficient to make the data fully anonymous. When data contains complex or unique descriptions of individuals, it may be practicable for others to identify them even if the data does not contain any obvious identifiers. For example, if the data is related to a small group of people, such as a certain class of students, individuals may be reasonably ascertained if certain indirect identifiers, such as their age, residence, years attended, academic results on specific subjects/areas, are kept.

Furthermore, with the advancement of information technology, it may be possible for the data user or any third parties to ascertain or reasonably ascertain the identities of individuals using other publicly available information. To prevent this, data users must consider carefully whether or not to release the anonymised data to third-parties or the public.

Data users must realise that using anonymisation instead of erasure entails the risk that individuals may be re-identified from the data in the future. In this era of Big Data, there has been growing concerns whether in the case of very large databases it will still be possible to genuinely and effectively anonymise individuals. Data users must make sure that the benefits of keeping anonymised data outweigh the potential risk that personal data may be used to re-identify individuals, and that the impact such re-identification would have on the individuals. For this reason, data users must review regularly whether anonymised data can be re-identified and take appropriate action to protect personal data.

Legal Requirements related to Personal Data Erasure

Section 26 of the Ordinance provides that a data user must take all practicable steps to erase personal data held when the data is no longer required for the purpose (including any directly related purpose) for which it was used, unless any such erasure is prohibited under any law or it is in the public interest not to have the data erased.