APPA Technology Working Group

GUIDE TO Getting Started with Anonymisation

Published June 2025

Introduction

This guide provides an overview of basic anonymisation concepts and practical steps that can be put in place to enable organisations to kickstart their anonymisation journey, starting with structured, textual and non-complex datasets. We hope this guide will allow readers to develop a useful foundational understanding of anonymisation before consulting more advanced resources and where it exists, more specific guidance from their jurisdictions.

Proper anonymisation requires both good knowledge of the data context and competency with the technicalities of anonymisation. Where the anonymisation is deemed complex or the data controller does not have the necessary level of skills, the data controller should consider engaging an expert to perform the anonymisation. It is important to note that anonymisation and re-identification techniques are evolving areas of research and new methodologies are periodically published. Data controllers who plan to implement anonymisation should survey the latest developments or consult experts in the field.

It is also recommended to refer to the ISO standard titled 'Information Security, Cybersecurity and Privacy Protection – Privacy Enhancing Data De-identification Framework' (ISO/IEC 27559:2022[1]). This standard recognises that anonymisation involves not only the data itself but also the context in which data is shared and used, as well as the governance practices in place. Adopting these best practices can help organisations effectively manage the risk of re-identification while maintaining the utility of anonymised data.

Disclaimer: This guide is written for informational purposes only. It discusses anonymisation from a technical perspective, as opposed to a legal or policy perspective. It does not contain legal advice, nor do the views expressed in it necessarily reflect the official policy or position of individual Asia Pacific Privacy Authorities (APPA) or APPA Technology Working Group (TWG) members. This guide is not exhaustive in dealing with all the issues relating to anonymisation. It is not a substitute for regulatory guidance from respective jurisdictions. Organisations should refer to regulatory guidance, where it exists, to ensure compliance with relevant data protection regulations.

[1] *It is important to note that ISO/IEC 27559 was written under the assumption of a strict binary distinction between information that is subject to privacy laws (i.e. 'personal' information) and information that is outside the scope of privacy laws (i.e. 'anonymised' information). While first-generation privacy laws worked under this same assumption, more modern privacy laws tend to use a more flexible three-fold distinction between personal, 'de-identified' (or 'pseudonymised') and anonymised information, where de-identified (or pseudonymised) information is still subject to privacy laws. Given this discrepancy, it is unclear whether and under what circumstances information 'anonymised' according to ISO/IEC 27559 should be considered de-identified (or pseudonymised) under modern privacy frameworks.*

What is Anonymisation?

At a technical level, anonymisation[2] is the process of converting personal data into data that can no longer be used to identify an individual[3], either alone or in combination with other information, by taking reasonable measures that take into account the current state of the art.

Why Anonymise Data?

Generally, data that has been anonymised is not considered personal data. However, it is important to recognise that the process of anonymisation requires rigorous assessment, risk management, and ongoing governance as outlined in the ISO/IEC 27559 Privacy Enhancing Data De-identification Framework. This includes context assessments, data assessments, identifiability assessments, and the implementation of robust mitigation measures to ensure that the risk of re-identification remains below a predefined tolerance level. Continuous monitoring and adherence to established anonymisation practices are critical to maintaining the non-personal status of anonymised data.

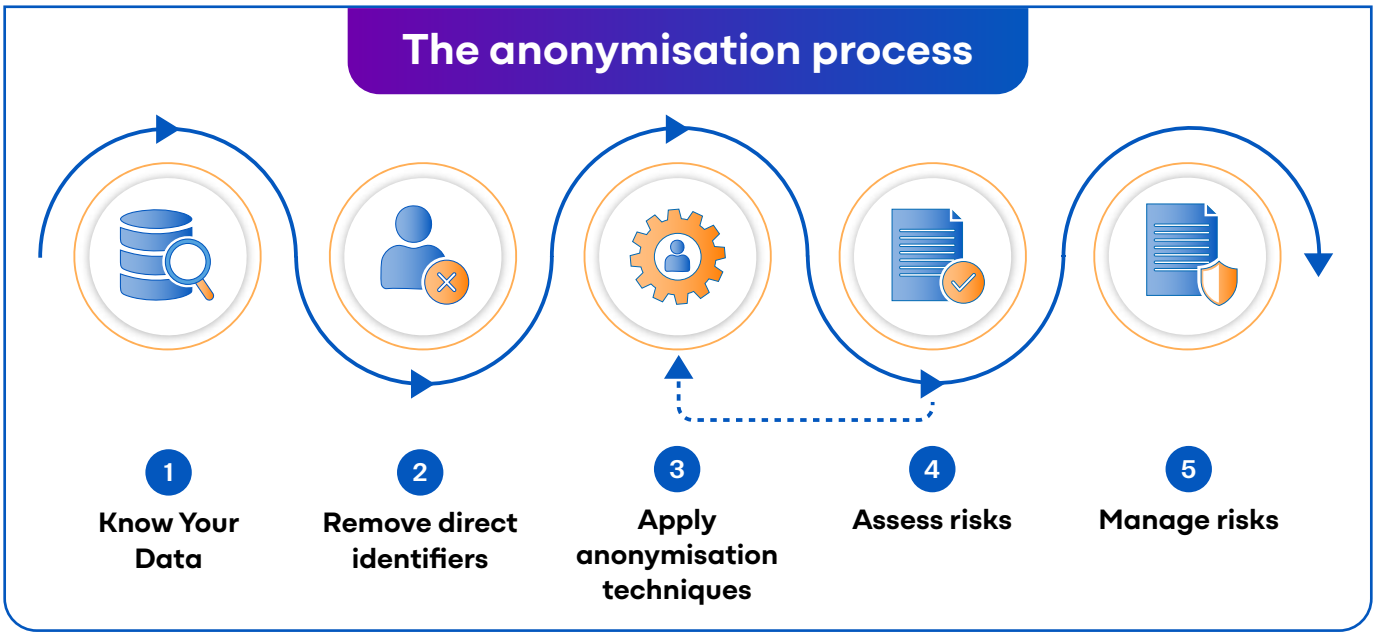
Best practices and standards, such as those outlined in ISO/IEC 27559, consider anonymisation as a risk-based process that includes the application of anonymisation techniques to the data, as well as the implementation of other privacy and security measures to mitigate re-identification risks[4]. This guide suggests practical steps to assist organisations in assessing and reducing such risks while still obtaining useful data.

By anonymising data, for example, when sharing data with external entities, organisations can gain insights from data while providing protection to data subjects. It may also be a requirement under the data protection laws for organisations to either destroy or anonymise personal data when there is no longer a valid reason to retain the personal data.

[2] Anonymisation is referred to as de-identification in some countries' data protection laws while some definitions may consider de-identification as only the removal of direct identifiers. Also, some jurisdictions may consider that if there are still risks to be managed, such data can only be referred to as pseudonymised data and not anonymised data. Legal standards for what are considered 'anonymised' and 'de-identified' data can vary across data protection jurisdictions.

[3] Step 4 in this document discusses how to assess re-identification risks.

[4] Steps 1 to 5 in this guide would be applicable for organisations under such jurisdictions.



The above diagram is a simplified[5] overview of the suggested anonymisation process.

Step 1: Know Your Data

A personal data record is made up of data attributes that have varying degrees of identifiability and sensitivity to an individual. Anonymisation typically involves removal of direct identifiers and modification of indirect identifiers. Target attributes are usually left unchanged.

> **Direct identifiers** are data attributes that are generally unique to an individual and can be used as key data attributes in the data record to re-identify an individual. Common examples of direct identifiers are name and national identity number.

> **Indirect identifiers** are data attributes that are generally not unique to an individual but combinations of them may be unique and then used to re-identify an individual in the data record when combined with other information, including direct identifiers. Common examples of indirect identifiers are birth date, gender and postal code.

[5] *The steps are not intended to be prescriptive but to provide a general guide on the anonymisation process. Organisations may tweak the steps based on their context and internal processes. E.g. risk assessment can also be done first before anonymisation techniques are applied.*

Target attributes are the remaining data attributes that contain the main utility of the dataset. In the context of assessing the adequacy of anonymisation, this data attribute may be sensitive in nature and may result in a high potential for adverse effect to an individual if disclosed. These data attributes are usually not publicly available or easily accessible. An example of a target attribute could be an individual's health diagnosis. Extra consideration and caution should be given where such target attributes may be easily accessible or otherwise available, and to categorise such data attributes as indirect data attributes instead.

Step 2: Remove direct identifiers

Remove all direct identifiers. If needed, assign a pseudonym to each record. The pseudonyms should be unique for each direct identifier. Assignment of pseudonyms should also be robust, meaning that they should not contain identifiable information and not be reversible by unauthorised parties through guessing or computing the original direct identifier values from the pseudonyms.

Step 3: Apply anonymisation techniques

In this step, apply anonymisation techniques to the indirect identifiers so that they cannot be combined with other datasets that may contain additional information to re-identify individuals. Do note that application of these techniques will modify the data values and may affect the utility of the anonymised data. Anonymisation techniques include data suppression, masking, generalisation, adding noise to data, sampling and data swapping. ISO/IEC 20889 titled 'Privacy Enhancing Data De-identification Terminology and Classification of Techniques' provides a comprehensive list of possible anonymisation techniques.

It is important to choose technique(s) that are appropriate to the dataset and to the way the data will be used. It is the responsibility of organisations to ensure that they choose technique(s) that are suitable for the circumstances. Different techniques have benefits and drawbacks, both for privacy and for utility, and organisations should be aware of these to make informed and deliberate choices about which technique(s) to use.

Step 4: Assess re-identification risks

It is useful to compute the re-identification risks of anonymised data. Methods such as *k*-anonymity[6] can be used to compute the re-identification risks. *k*-anonymity may not be suitable for all datasets. Other approaches/tools like Special Unique Detection Algorithms (SUDA) and μ-Argus may also be considered by organisations to assess the re-identification risk of shared datasets.

k-anonymity is a simple method to compute the re-identification risk level of a dataset where such dataset is non-complex and does not have large numbers of data attributes. It basically refers to the smallest number of identical records that can be grouped together in a dataset. The smallest group is usually taken to represent the worst-case scenario in assessing the overall re-identification risk of the dataset. Generally, only indirect identifiers are considered for *k*-anonymity computation. A higher *k*-anonymity value means there is a lower risk of re-identification while a lower *k*-anonymity value implies a higher risk of re-identification. Figure 1 below provides a simple illustration of a dataset with three groups of identical records. The *k* value of each group ranges from 2 to 4. Overall, the dataset's *k*-anonymity value is 2, reflecting the lowest value (highest risk)[7] within the entire dataset.

Postal code	Age	Favourite show	
22xxxx	21 to 25	*Emily in Paris*	*k*=2
22xxxx	21 to 25	*Emily in Paris*	
10xxxx	41 to 45	*Brooklyn Nine-Nine*	*k*=4
10xxxx	41 to 45	*Brooklyn Nine-Nine*	
10xxxx	41 to 45	*Brooklyn Nine-Nine*	
10xxxx	41 to 45	*Brooklyn Nine-Nine*	
58xxxx	56 to 60	*Attenborough's Life in Colour*	*k*=3
58xxxx	56 to 60	*Attenborough's Life in Colour*	
58xxxx	56 to 60	*Attenborough's Life in Colour*	

Overall *k*=2

Figure 1: Illustration of *k*-anonymity

[6] *In general, the sufficiency of the anonymisation process is evaluated on a case-by-case basis. Singapore's Personal Data Protection Commission recommends a k value of at least 5 to be considered sufficiently anonymised, together with relevant safeguards. Also, k-anonymity is mainly used to protect against linking and singling attacks. Extensions to k-anonymity, such as l-diversity and t-closeness can be considered to protect against other attacks such as inference attacks.*

[7] *Focusing on the highest risk is the more conservative risk approach of looking at the maximum risk of re-identification within the dataset. There are also other approaches such as average risk and strict average risk.*

A 'motivated intruder' test[8] can be conducted to assess the residual risks of re-identification after anonymisation techniques have been applied. This test considers if individuals can be re-identified from anonymised data by someone who is motivated, reasonably competent, has access to public or private linkable data or information (e.g. the Internet, commercially available datasets and published information such as public directories) and employs standard investigative techniques (e.g. inferences and data linking).

Organisations should use their assessments of re-identification risk to ensure their data is sufficiently anonymised. This may require that organisations adjust their technique(s), apply additional measures, revise the scope of the dataset, remove outliers, etc. Hence, it may be necessary to go back to Step 3 or even earlier steps and repeat this looping until the results of Step 4 are satisfactory, i.e. the data is sufficiently anonymised.

Step 5: Manage re-identification risks

Mitigation measures serve to manage any residual risk after anonymisation techniques have been applied to data. Generally, stronger mitigation measures will be required for anonymised data with higher residual risk (e.g. lower *k*-anonymity values). Organisations should also consider the potential degree of harm to individuals in the case of re-identification in determining the mitigation measures to be implemented.

Mitigation measures generally include security measures that ensure the shared anonymised data can only be accessed by authorised users, as well as legal and/or governance measures that ensure that the data is only used in the intended ways.

There should also be mitigation measures to secure the identity mapping or linking information of the anonymised data to personally identifiable data, should the data controllers choose to retain such information.

While the application of mitigation measures may be viewed as an anonymisation technique, it is also possible to view them as an extension of data protection/privacy laws. If after Step 4, the risk of re-identification is not low enough for the data to be considered anonymised, then the data would still be considered identifiable. This means that data protection/privacy laws would continue to apply to it. In certain jurisdictions, the application of mitigation measures would then be viewed as a condition of rendering the data pseudonymised, as opposed to anonymised, while other jurisdictions may consider the application of such measures collectively as part of risk-based approach for anonymisation. Organisations should consult their respective jurisdictions' regulations for the interpretation.

[8] *Highlighted in the Information Commissioner's Office (UK)'s Code of Practice, Anonymisation: Managing Data Protection Risk Code of Practice.*

Useful considerations from ISO/IEC 27559

Other than the 5-step process described above, organisations can also refer to ISO/IEC 27559 which provides a useful framework and considerations for context assessment, data assessment, identifiability assessment and mitigation, and governance.

Context Assessment: This involves evaluating the environment and circumstances in which data is made available to data recipients. It includes threat modelling, assessing security and privacy practices as well as evaluating motives and capacity to re-identify.

Data Assessment: This focuses on understanding the features of the data and modelling potential attacks that could exploit vulnerabilities. It covers data features, attack modelling, and the selection of data privacy models to quantify identifiability.

Identifiability Assessment and Mitigation: This involves assessing the probability of an attack and the likelihood of successful identification of a subject. The framework outlines methods for quantifying identifiability and suggests mitigation measures, such as reconfiguring the environment or transforming the data to reduce identifiability.

De-identification/Anonymisation Governance: Governance includes establishing principles, policies, and procedures to manage data processing activities and ensure compliance with data security and privacy standards. It also covers roles and responsibilities, monitoring risks and handling unintended disclosures.

Other recommended practices

Periodic reviews should be conducted to ensure the risk of re-identification remains low over time. Organisations need to ensure that no new technologies and techniques have evolved, or no new dataset has been made accessible or publicly available to allow re-identification of the anonymised data. Reviews will also ensure that risk mitigation measures are effective and working as intended, and still appropriate if organisational circumstances change.

Whether or not data protection authorities consider a set of data to be anonymised generally depends on the likelihood of re-identification. Depending on jurisdictions, data protection authorities could also consider the safeguards (including technical, governance and contractual measures) and the anonymisation process used. It is, hence, useful to keep records of such information when anonymisation is performed.

Annex A: Resources on Anonymisation

ISO/IEC

ISO/IEC has published the following standards, among others, that are related to anonymisation.

Resource	Description
ISO/IEC 20889:2018 – Privacy enhancing data de-identification terminology and classification of techniques	The standard specifies terminology, a classification of de-identification techniques according to their characteristics, and their applicability for reducing the risk of re-identification. Available at https://www.iso.org/standard/69373.html
ISO/IEC 27559:2022 – Information security, cybersecurity, and privacy protection – Privacy enhancing data de-identification framework	The standard provides a framework for identifying and mitigating re-identification risks and risks associated with the lifecycle of de-identified data. It can help organisations determine how a de-identification process is implemented in practice. It is a standard based on commonalities for broad adoption and best practices. It takes a risk-based approach. Available at https://www.iso.org/standard/71677.html

Australia (Commonwealth)

The Office of the Australian Information Commissioner (OAIC) has guidance relating to de-identification under Australia's national privacy laws. Ensuring that information has been 'de-identified' for the purpose of the *Privacy Act 1988* (Cth) requires entities to adopt an approach similar to 'anonymisation'.

The De-Identification Decision-Making Framework, jointly published by the OAIC and CSIRO's Data61, assists organisations to de-identify their data effectively. The De-Identification Decision-Making Framework is a practical and accessible guide for Australian organisations that handle personal information and are considering sharing or releasing it to meet their ethical responsibilities and legal obligations.

The OAIC also has guidance on De-identification and the Privacy Act, which includes general advice about de-identification and protecting privacy to maximise the utility and value of data while safeguarding privacy.

Resource	Available at
De-identification Decision-Making Framework	https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/handling-personal-information/de-identification-decision-making-framework
De-identification and the Privacy Act	www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/handling-personal-information/de-identification-and-the-privacy-act

Victoria, Australia

The Office of the Victorian Information Commissioner (OVIC) provides a suite of free resources on its website, covering:

- an entry level introduction to de-identification – what it means, how it works, as well as the risks and challenges involved,
- practical tips on what to consider when de-identifying information, and how to manage the risks of re-identification and
- more in-depth guidance on de-identification techniques and the limitations of these approaches in protecting unit-record level personal information.

In OVIC's jurisdiction, 'de-identification' is the word used to describe 'anonymisation', as defined in this guide.

Resource	Available at
An introduction to de-identification	https://ovic.vic.gov.au/privacy/resources-for-organisations/an-introduction-to-de-identification/
De-identification: An exercise in risk management	https://vimeo.com/722443647
Limitations of de-identification	https://ovic.vic.gov.au/privacy/resources-for-organisations/the-limitations-of-de-identification-protecting-unit-record-level-personal-information/

South Korea

South Korea's Personal Information Protection Commission (PIPC) explains the governance of pseudonymised information through its 'Pseudonymised Information Processing Guidelines' amended in 2022.

The Korean Personal Information Protection Act (PIPA) stipulates pseudonymised information as personal information. PIPC has published the guidelines for a better understanding of the public's processing, combination, exportation and safety measures of pseudonymised information.

The guidelines specify precautions for each pseudonymised information processing process and how to protect the rights of data subjects through technical, administrative, and physical protection measures.

Additionally, in response to the growing demand to use unstructured data such as images and video recordings, which became available through advancement of AI technology, the released Guidelines (February 2024) includes detailed cases and scenarios for different fields including healthcare, traffic and chatbot.

Resource	Available at
Brief Overview of Pseudonymization	https://www.pipc.go.kr/eng/user/lgp/bnp/pseudonymization.do
Guidelines for Pseudonymizing Unstructured Data (PDF file. Abridged Eng. ver.)	https://www.pipc.go.kr/eng/user/lgp/law/ordinancesDetail.do?bbsId=BBSMSTR_000000000005&nttId=2699#none
Guidelines for Pseudonymizing Data (2022 ver.)	※Korean only https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS217&mCode=G010030000&nttId=8000

Japan

The Personal Information Protection Commission (PPC) has published guidelines regarding the handling of anonymised personal information under the Act on the Protection of Personal Information (APPI) to support proper and effective implementation of measures for personal information protection by organisations. PPC has further published a report containing more details on the handling of anonymised personal information to facilitate self-regulatory efforts by organisations. These materials also address pseudonymised personal information, which is stipulated in the APPI as having a different nature from anonymised personal information.

Resource	Available at
Guidelines	※Japanese only https://www.ppc.go.jp/personalinfo/legal/#anc_Guide
Report by the Personal Information Protection Commission Secretariat	(Edition on Legal system) ※Japanese only https://www.ppc.go.jp/files/pdf/report_office_seido2205.pdf (Edition on Case study) ※Japanese only https://www.ppc.go.jp/files/pdf/report_office_zirei2205.pdf

Singapore

The Personal Data Protection Commission (PDPC) has published advisory guidelines to explain how anonymisation is defined under the Personal Data Protection Act (PDPA) and what are the requirements for data to be considered anonymised. PDPC has also published a technical guide on anonymisation which provides suggestions on implementation aspects. Finally, the data anonymisation tool is a free tool that complements the technical guide, and is useful for readers of the guide in learning about anonymisation and in anonymising simple datasets.

Resource	Available at
Advisory Guidelines on the Personal Data Protection Act for Selected Topics (Chapter 3 - anonymisation)	https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/advisory-guidelines/ag-on-selected-topics/advisory-guidelines-on-the-pdpa-for-selected-topics-(revised-may-2024).pdf
• *Guide to Basic Anonymisation* • *Data anonymisation tool*	English version: https://www.pdpc.gov.sg/Help-and-Resources/2018/01/Basic-Anonymisation Spanish version (published by AEPD, the Spanish DPA): https://www.aepd.es/es/documento/guia-basica-anonimizacion.pdf https://www.aepd.es/es/descargas/herramienta-anonimizacion-pdpc
[video] *Introduction to PDPC's Data Anonymisation Tool*	www.youtube.com/watch?v=qlnYRI5VwQQ

Annex B: Case Study

This section provides a hypothetical example to illustrate the steps described above.

The scenario presented in this example is a gym, Vivogym, which would like to share anonymised data with a marketing partner, The Pink Group, to profile its customers and create a new marketing campaign.

The following table shows an excerpt of the original customer data from Vivogym's database. All data used for this example is fictitious. In this guide, we show 10 records from the dataset.

S/N	Name	Birth Date	Postal Code (Singapore)	Weight (kg)	Height (m)	Most Time Spent in Last 6 Months
1	Demond Nix	9/12/1996	322607	52	1.60	Treadmill
2	Treyvon Coker	24/12/1998	335662	56	1.75	Pilates
3	Jarred Zielinski	3/10/1995	355895	72	1.65	Swim
4	Rolando Toth	10/12/1996	359383	79	1.67	Spin
5	Benny Beckman	8/12/1996	316551	65	1.60	Weights
6	Dakota Birch	5/9/1997	326125	66	1.75	Weights
7	Jacques Colburn	4/9/1995	339035	72	1.68	Kickboxing
8	Kendyl Fletcher	25/10/1999	346214	79	1.72	Weights
9	Keegan Knapp	26/10/1997	346204	59	1.62	Pilates
10	Yoselin Provost	4/9/1995	324946	61	1.75	Weights
(many more records which are not listed in this document due to space constraints)						

Step 1: Know Your Data

In this example, Vivo Gym classifies the data attributes in the following way:

Data Attribute	Name	Birth Date	Postal Code (Singapore)	Weight (kg)	Height (m)	Most Time Spent in Last 6 Months
Classification	Direct identifier	Indirect identifier	Indirect identifier	Indirect identifier	Indirect identifier	Target attribute

Step 2: Remove direct identifiers

In this example, the only direct identifier is the customer's name. This is removed from the dataset.

S/N	~~Name~~	Birth Date	Postal Code (Singapore)	Weight (kg)	Height (m)	Most Time Spent in Last 6 Months
1	~~Demond Nix~~	9/12/1996	322607	52	1.60	Treadmill
2	~~Treyvon Coker~~	24/12/1998	335662	56	1.75	Pilates
3	~~Jarred Zielinski~~	3/10/1995	355895	72	1.65	Swim
4	~~Rolando Toth~~	10/12/1996	359383	79	1.67	Spin
5	~~Benny Beckman~~	8/12/1996	316551	65	1.60	Weights
6	~~Dakota Birch~~	5/9/1997	326125	66	1.75	Weights
7	~~Jacques Colburn~~	4/9/1995	339035	72	1.68	Kickboxing
8	~~Kendyl Fletcher~~	25/10/1999	346214	79	1.72	Weights
9	~~Keegan Knapp~~	26/10/1997	346204	59	1.62	Pilates
10	~~Yoselin Provost~~	4/9/1995	324946	61	1.75	Weights
(many more records which are not listed in this document due to space constraints)						

Step 3: Apply anonymisation techniques

The gym decides how to anonymise the various indirect identifiers, as described in the following table:

Indirect Identifier	Anonymisation Technique
Birth Date	Generalise from an exact date to just the year of birth.
Postal Code (Singapore)	Mask the last 4 digits of the 6-digit postal code. This changes the value that can possibly point to a specific residential unit in some cases, to a less granular district specification.
Weight (kg)	Combine the weight and height into a Body Mass Index (BMI) value, then generalising into numerical ranges of 10 units.
Height (m)	

After anonymisation, the dataset looks like this:

S/N	Birth Date	Postal Code (Singapore)	BMI	Most Time Spent in Last 6 Months
1	1996	32****	20 - 29	Treadmill
2	1998	33****	10 - 19	Pilates
3	1995	35****	20 - 29	Swim
4	1996	35****	20 - 29	Spin
5	1996	31****	20 - 29	Weights
6	1997	32****	20 - 29	Weights
7	1995	33****	20 - 29	Kickboxing
8	1999	34****	20 - 29	Weights
9	1997	34****	20 - 29	Pilates
10	1995	32****	10 - 19	Weights
(many more records which are not listed in this document due to space constraints)				

Step 4: Assess re-identification risks

The gym then groups similar records in the dataset, i.e. records having the same birth date, postal code and BMI. Similarity of records is assessed without taking into consideration the data attribute "Most Time Spent in Last 6 Months", which is classified as a target attribute and is not used for *k*-anonymity computation.

S/N	Birth Date	Postal Code (Singapore)	BMI	Number of records in dataset with same indirect identifiers (birth data, postal code and BMI), i.e. *k*	Most Time Spent in Last 6 Months
1	1996	32****	20 - 29	5	(unchanged values)
2	1998	33****	10 - 19	6	(unchanged values)
3	1995	35****	20 - 29	5	(unchanged values)
4	1996	35****	20 - 29	5	(unchanged values)
5	1996	31****	20 - 29	6	(unchanged values)
6	1997	32****	20 - 29	7	(unchanged values)
7	1995	33****	20 - 29	5	(unchanged values)
8	1999	34****	20 - 29	4	(unchanged values)
9	1997	34****	20 - 29	6	(unchanged values)
10	1995	32****	10 - 19	5	(unchanged values)
(many more records which are not listed in this document due to space constraints)					

The *k*-anonymity value can be computed by specialised tools[9], or using spreadsheet software and calculating the number of records containing the same indirect identifiers.

In this example, initially the overall dataset's *k*-anonymity value is 4, reflecting the group of records with the lowest *k* value (highest risk) within the entire dataset. If the gym decides to improve the overall *k* value to be 5 instead, it can consider removing the outlier records (in red, with *k* value less than 5) to improve the *k*-anonymity value from 4 to 5.

The gym assesses the re-identification risks for the record by conducting the 'motivated intruder' test to assess the likelihood of re-identification from the anonymised data. The gym also takes into account any potential harms that might arise to the individuals if a re-identification occurs, as well as, based on the guidance from the jurisdiction that it is operating under. Based on the above, the gym will repeat steps 3 and 4 until a reasonably high level of *k*-anonymity value is achieved while still enabling the dataset to be useful for its purpose (profiling of customers).

[9] *There are various free and commercial anonymisation tools available.*

Step 5: Manage re-identification risks

The gym implements the following safeguards to ensure that any residual risk of re-identification is mitigated or reasonably minimised:

Contractual safeguards: In the contract with the marketing company:

- Restrict the use of the anonymised data to only intended purposes and for intended personnel,
- Prohibit deliberate attempts at re-identification, and
- Require deletion of the anonymised data after the intended purposes have been achieved or when the data would no longer be used.

Technical safeguards:

- Implement access control at the marketing company to control and limit access to the anonymised dataset to authorised employees, and
- Delete the anonymised data after the data has been used. This can be scheduled ahead of time.

Governance safeguards:

- Keep records of the anonymised dataset and details of the anonymisation process, as well as a record of data sharing activities.

Acknowledgements

This guide was developed by the Technology Working Group (TWG) of the Asia Pacific Privacy Authorities (APPA), which consists of the following members:

- Office of the Victorian Information Commissioner, Victoria, Australia (OVIC)
- Office of the Privacy Commissioner, Canada (OPC)
- Office of the Information and Privacy Commissioner, British Columbia, Canada (OIPC)
- Office of the Privacy Commissioner for Personal Data, Hong Kong, China (PCPD)
- Personal Data Protection Bureau, Macao, China (PDPB)
- The Personal Information Protection Commission, Japan (PPC)
- Office of the Privacy Commissioner, New Zealand (OPC)
- Personal Data Protection Commission, Singapore (PDPC)
- Korea Personal Information Protection Commission, South Korea (PIPC)


APPA
Asia Pacific Privacy Authorities