



Data Ethics for Small and Medium Enterprises

Preamble

In a data-driven economy, small and medium enterprises (“SMEs”), including tech start-ups, increasingly use personal data of customers as an asset in operating and advancing their businesses. The rapid development in information and communications technology, particularly advanced data processing activities (including big data analytics and artificial intelligence), present business opportunities but at the same time challenges privacy and data protection.

It is not in dispute that personal data belongs to the data subjects. SMEs that derive benefits from personal data should ditch the mindset of conducting their operations to merely meet the minimum regulatory requirements only. They should instead be held to a higher ethical standard that meets stakeholders’ expectations alongside the requirements of laws and regulations. Data ethics can therefore bridge the gap between legal requirements and stakeholders’ expectations.

In fact, ethical use of personal data makes good business sense. **Respectful, beneficial** and **fair** use of customers’ personal data can improve business reputation and enhance stakeholders’ confidence. This leaflet aims to help SMEs understand the means to implement data ethics. When SMEs develop an assessment process to ensure that personal data is processed ethically, individuals will have greater confidence in their data being protected. In turn, customers’ trust will grow and become a competitive edge of the SMEs. Under the trend of service and

product personalisation and mobilisation in the future smart society, enterprises will benefit by grasping and implementing data ethics.

Three Core Values of Data Ethics

SMEs are encouraged to handle personal data pursuant to three core values, namely being **Respectful, Beneficial** and **Fair**.

Respectful¹

- SMEs should be accountable for conducting advanced data processing activities
- SMEs should consider the expectations of the individuals to whom the data relate and/or impacted by the data use
- SMEs should consider all parties that have interests in the data
- Decisions made about an individual and the relevant decision-making process should be explainable and reasonable
- Individuals should be able to make inquiries, obtain explanation and appeal against decisions on the advanced data processing activities that impact them

¹ The Respectful value is consistent with Data Protection Principles (DPPs) 1, 3, 5 and 6 in Schedule 1 to the Personal Data (Privacy) Ordinance (Chapter 486 of the Laws of Hong Kong).

Beneficial²

- To define, identify and assess the benefits and potential risks of the advanced data processing activities which have potential impact on individuals
- To implement measures to mitigate all the identified risks and balance the interests of different parties, not to consider the benefits of enterprises alone

Fair³

- Advanced data processing activities must avoid actions that seem inappropriate or might be considered offensive or causing distress
- Unequal treatment or discrimination should be prohibited
- The accuracy and relevance of algorithms, models and datasets used in decision-making should be regularly reviewed to reduce error, uncertainty, bias or discrimination
- Advanced data processing activities should be consistent with the SMEs' ethical values

Ethical Data Impact Assessment

SMEs are advised to conduct Ethical Data Impact Assessment before deciding to pursue an advanced data processing activity by answering the following questions. Through the assessment, SMEs can understand their ethical responsibilities for data protection and find out the impact of their data-driven activities on their stakeholders' rights and interests.

Purpose of the activity

Business objective and purpose of the data activity

- What is the business need/objective for this data activity?
- Is this data activity an expansion of a previous activity? If a previous assessment has been done, what has changed in this data activity and the reasons for the change?

Accountability for the data activity

- Who needs to be involved in making decision regarding the data activity? Who has ultimate decision-making authority for the data activity?
- Who is accountable for the various phases of the data activity?

Legal and other obligations regarding data collection, analysis and use

- What laws, regulations, policies and contractual obligations apply to the collection, analysis, use and transfer of data?
- Does the data activity comply with the SMEs' internal policies?
- How will the legal and other obligations be managed and satisfied?

A full understanding of the data, its use and parties involved

The nature of the data

- What specific types of data that will be collected, tracked, transferred, used, stored, processed or disposed of?
- Is the data personally identifiable? Is data re-identification possible from anonymised data?
- Is the data (e.g. race, ethnic origin, sexual orientation, physical or mental health) or its anticipated use sensitive?

² The Beneficial value is consistent with the reduction of risk concept expressed in DPP4.

³ The Fair value is consistent with DPPs 1(2), 2(1) and 3.

The sources of the data to be used in the data activity

- Is the data provided by the individual, observed⁴, derived⁵ or inferred⁶?
- Are the sources of the data from a legitimate entity? Are the sources reliable and permissible for the purpose of the activity?

The accuracy of the data

- Is the data accurate enough for the purpose of the data activity?

The governance of the data

- If the data has been collected by, shared with and/or received from others, do those parties have authority to share and to transfer?

Impact on parties, in particular individuals

Identify all the impacted parties and the impacts on those parties

Benefits

- What are the benefits to the individual, groups of individuals and society?
- How significant are the benefits?
- Are the benefits likely to occur? How likely?
- What are the benefits to the entity itself?

Risks

- What are the risks to the individual, groups of individuals and society?
- Is it foreseeable that the potential data analytical insights or the data activity might seem inappropriate, discriminatory, offensive, causing distress or humiliation to individuals and other stakeholders?
- What is the impact of inaccurate data?
- How significant are the risks?

Controls

- What kinds of technical and procedural safeguards (e.g. encryption and de-identification of data) will be implemented to prevent and mitigate risks?

- Is there a less data-intensive way to achieve the goals of the data activity?
- If data is to be shared with third parties, does such use match with the original collection purpose of the data? What measures will be adopted to ensure that the data will be properly protected by the third parties?
- How effective are these controls and safeguards in reducing risks?

Whether an appropriate balance of benefits and mitigated risks supports the data-processing activity

Outcome

- Have the interests, rights and expectations of individuals been duly considered?
- Is it necessary to take the risks arising from the data activity? Are the risks proportionate to the benefits? Have the risks been mitigated to the greatest extent practicable?
- After considering all the above factors, is the activity a “go” or “no go”, or should some aspects of the activity be modified to reduce the residual risk?

Approval

- Have those persons who have an ultimate decision-making authority on the data activity and are accountable for various phases of the data activity been involved in the decision?

Conclusion

The Personal Data (Privacy) Ordinance and regulation should not hinder innovation and technology as well as economic development. Fundamentally, there is interactive relationship between technology development and application and personal data privacy rights. SMEs are expected to implement data ethics in their daily operations, and to fully reap the benefits of the data-driven economy while protecting and respecting the fundamental human rights (including the right to privacy), interests and freedoms of individuals.

⁴ Created as the result of individuals being observed or tracked.

⁵ Created in a mechanical fashion from other data and becomes a new data element related to the individual.

⁶ Product of a probability-based analytic process.



Download this publication

SME Hotline : (852) 2110 1155
SME Email : sme@pcpd.org.hk
Enquiry Hotline : (852) 2827 2827
Fax : (852) 2877 7026
Address : Room 1303, 13/F, Sunlight Tower, 248 Queen's Road East, Wanchai, Hong Kong
Email : enquiry@pcpd.org.hk



This publication is licensed under a Creative Commons Attribution 4.0 International (CC BY 4.0) licence. In essence, you are free to share and adapt this publication, as long as you attribute the work to the office of the Privacy Commissioner for Personal Data, Hong Kong. For details, please visit creativecommons.org/licenses/by/4.0.

Disclaimer

The information and suggestions provided in this publication are for general reference only. They do not serve as an exhaustive guide to the application of the law. The Privacy Commissioner makes no express or implied warranties of accuracy or fitness for a particular purpose or use with respect to the information and suggestions set out in this publication. The information and suggestions provided will not affect the functions and powers conferred upon the Privacy Commissioner under the Personal Data (Privacy) Ordinance.

First published in April 2019