Malaysia eCommerce
Data Sharing Code of Practice

18 February 2022

Table of Contents

Section 1: Introduction

1.1. About the Code of Practice

eCommerce is defined as the act of purchasing and selling products online. According to Malaysia's Department of Statistics, eCommerce recorded a double-digit contribution of 11.5% to Malaysia's GDP in 2020 compared with 8.5% in 2019. This was the first time a double-digit growth was achieved. In 2021, there was an increase in eCommerce income year over year (YoY), at 23.1%, from January to September, which amounted to RM801.2 billion[1].

This number is expected to increase in the next few years, as the National eCommerce Strategic Roadmap 2.0 (NESR 2.0) aims to assist 875,000 micro, small and medium-sized enterprises (MSMEs) adopt eCommerce by 2025. A similar endeavour was done in 2020, wherein eCommerce was adopted by 489,000 MSMEs[2]. The NESR 2.0 has three key objectives that are aligned with Malaysia Digital Economy Blueprint's (MyDIGITAL) plans, with the aim of enhancing economic competitiveness through digitalisation and establishing an inclusive digital society. These three objectives are increasing eCommerce adoption and growth, bolstering policy and regulatory environment, and boosting ecosystem development.

eCommerce platform users share data such as the time they spent on browsing certain products, frequency of site visits, payment details, identity data, and contact data, among others. This user data is shared with eCommerce partners such as logistics and payment partners. As data sharing is prevalent in eCommerce, and given the huge potential of eCommerce in Malaysia, it is important for eCommerce value chain players to have good data ethics.

Sensitive and confidential data collected by eCommerce companies should be covered by well-documented privacy policies to ensure that data sharing along the eCommerce value chain is conducted in a fair and transparent manner. This will in turn increase confidence in data originators, such as eCommerce platform users, to share data in a setting where data privacy and data security are ensured. The benefit of increased trust and comfort when browsing on eCommerce platforms would be an increase in sales quantity as well as in the value of each transaction.

Malaysia's eCommerce Data Sharing Code of Practice intends to provide actionable instructions when it comes to the sharing of data in the eCommerce value chain. This is for the benefit of all eCommerce value chain players, which means that it is easily adaptable to smaller and emerging eCommerce players in Malaysia, as different organisations may be at different maturity levels in terms of formulating internal data privacy policies.

[1] DOSM (2021). *Malaysia e-commerce income soared 17.1 per cent to RM279.0 billion in the third quarter 2021*. Retrieved from https://www.dosm.gov.my/v1/index.php?r=column/cthemeByCat&cat=473&bul_id=cmRYZ21sUVF4elBySHVWckhkMGU4Zz09&menu_id=b0pIV1E3RW40VWRTUkZocEhyZ1pLUT09#:~:text=CONTRIBUTION%20AND%20PERFORMANCE%20OF%20DIGITAL%20ECONOMY&text=0%20billion%20in%202020%2C%20a,of%20other%20industries%20(8.4%25)

[2] The Edge (2021). *MDEC targets 875,000 MSMEs to adopt e-commerce by 2025*. Retrieved from https://www.theedgemarkets.com/article/mdec-targets-875000-msmes-adopt-ecommerce-2025

1.2. Objectives of the Code of Practice

a) The objective of this code of practice is to facilitate an open and safe data sharing environment in the eCommerce sector by ensuring that all stakeholders in the eCommerce value chain have confidence in how their data is collected, used, and shared.

b) The code of practice aims to establish principles for the collection and usage of data around the following key areas:

   i. Increase awareness around the collection, use, and sharing of data.

   ii. Improve transparency, clarity, and honesty in the way data is collected, used, and shared.

   iii. Ensure fair and equitable collection, use, and sharing of data.

   iv. Build trust and confidence in the way data is collected, used, and shared.

c) This code of practice outlines broad suggestions and recommendations for stakeholders in the eCommerce value chain to have good data sharing practices.

d) Adherence to this code of practice is on a voluntary basis, but any eCommerce stakeholder that collects, uses, and shares data is highly encouraged to adopt the data sharing principles outlined in the code of practice.

1.3. Definitions

a) The code of practice covers three categories of data, namely:

   i. Public Data — Data from any source that relates to eCommerce or the stakeholders in the eCommerce value chain, which can be freely used, reused, and redistributed by anyone with no existing local, national, or international legal restrictions on access or usage.

   ii. Private Data — Data created by an organisation such as an eCommerce platform to be utilised for specific purposes such as logistics processing by a logistics service provider.

   iii. Personal Data — Data that is identifiable to an individual or organisation.

b) The code of practice aims to cover the eCommerce value chain, which consists of stakeholders such as eCommerce companies, logistics companies, payment partners, marketplace sellers, eCommerce platform users (e.g., customers and potential customers), and others. The role of the stakeholders in the eCommerce value chain varies depending on the activities they perform, and hence falls into the category of either a Data Provider, Data User, or Data Originator.

c) Data sharing refers to the disclosure of data from one or more organisations to another organisation(s), or the sharing of data among different parts of an organisation.

Table 1: Non-Exhaustive Examples of Data Sharing in the eCommerce Ecosystem

User & Marketplace Sellers to eCommerce Platform	
Identity data	Name, gender, date of birth
Contact data	Billing and delivery address, phone number, email address
Transaction data	Order details
Account data	Bank account details, credit card details, payment details
Usage data	Searched items
Technical data	Internet Protocol (IP) address
Marketing and communications data	Marketing preferences, chat history
eCommerce Platform to Third Parties	
Payment Service Providers Account data of customers and/or sellers	Bank account details, credit card details, payment details
Logistics, Shipping and/or Customs Contact data	Billing and delivery address, phone number, email address
Marketing Account data of customers and/or sellers	Marketing, survey, social media, customer service, data analytics, market or consumer research, installation services
eCommerce Platform to Users	
Marketing and communications data	Marketing from eCommerce players or third-party customer service providers
Delivery updates	Updates from logistics partner via platform
eCommerce Platform to Sellers (Including Overseas sellers)	
Contact data of customers	Name, billing and delivery address, phone number, email address
Transaction data of customers	Order details

Section 2: Code of Practice

2.1. Data Collection and Sharing

a) When collecting and sharing data between any parties within the eCommerce value chain, a data collection and sharing agreement will need to be established. The data collection and sharing agreement provides the following benefits:

   i. Helps eCommerce stakeholders have clarity on their roles in the data collection and sharing process.

   ii. Details out the purpose of data collection and sharing.

   iii. Details what happens to the data at each stage of collection and sharing.

   iv. Details any data collection and data sharing policies to be adhered to (e.g., Personal Data Protection Act 2010).

   v. Provides the data originator ownership of the data in terms of how the data is handled.

b) The data collection and sharing agreement has no set format; it is at the discretion of the stakeholders involved to determine the terms based on the scale and complexity of the data collection and sharing. The agreement is to be drafted in clear, concise language that is easy to understand.

c) The data collection and sharing agreement must take into consideration the following areas:

   i. All parties that will be involved in the data collection and sharing process.

   ii. The purpose of data collection and sharing.

   iii. Conditions for inclusion or exclusion of additional parties in the data collection and sharing process.

   iv. Details about the types of data that will be collected and shared. The types of data collected should be clearly defined and categorised and should be as detailed as possible to ensure clear communication to the data originator.

d) eCommerce websites must ensure that they have established their privacy policy pages that outline and specify the required details about the purpose and reach of the data being collected and subsequently shared. As an example, if an eCommerce company is collecting information from consumers such as their names, email addresses, and spending trends around particular products with the intention of sharing this information with an advertisement agency, then this must be explicitly stated.

e) eCommerce websites must ensure that details of cookies being utilised on the website are clearly mentioned in the cookies notice, including the purpose of cookie collection and the security measures taken to store these cookies. Users must be provided with the option to opt out of cookies tracking should they not wish to have their information stored.

f) In the event that an eCommerce website contains links to third-party providers or products that are not governed by the data sharing and privacy policy of the eCommerce website, this must be clearly stated in the privacy policy page as well as any data sharing agreement that is established. As an example, if an eCommerce website displays a link to a network device manufacturer's product page, which collects data from consumers if they were to access the page, then this must be explicitly stated in the eCommerce company's privacy policy page.

Relevant Existing Acts Referred

a) The Personal Data Protection Act 2010 (PDPA), in covering rights for personal data, provides the following provisions when it comes to data ownership:

   i. A data user should not process personal data unless consent has been provided by the data owner.

   ii. A data user can process personal data from a data originator within the boundaries of a contractual agreement with the data originator.

2.2. Data Rights and Privacy

a) To protect the rights of data originators, any data sharing contract that is drafted must include the right of access to information held by the data provider as well as the right to object and request for rectification and erasure. As an example, if an eCommerce company (data provider) is storing product information from a marketplace seller on its platform, the marketplace seller must be allowed access to this information along with the ability to update the information when required.

b) Consent must be obtained from the data originator before data can be collected and shared.

c) To provide protection for data that is shared, the following components should be built into any data sharing contract:

   i. Details on which datasets can and will be shared, to prevent irrelevant or excessive information being disclosed.

   ii. Option to opt out from any marketing communications.

   iii. Uniformity in terms of data that is recorded and shared. The agreement could include examples showing how to record or convert data items. For example, if data needed is the date of birth, the format should be specified as either ''DD/MM/YYYY'' or ''MM/DD/YYYY'', or other formats. Agreeing on the right format can facilitate ease of data sharing transactions.

iv. In the event that the data originator wishes to remain anonymous, data must be anonymised. Otherwise, the contract should specify the conditions when a data originator needs to be identifiable. For example, in an eCommerce website's privacy policy page, if data is shared to third-party marketing companies, it should state or provide an option that eCommerce platform users can choose to remain anonymous if they do not want their personal data to be shared.

v. Particularise the procedures for dealing with data access requests for a data originator. For example, if a marketplace seller uploaded data related to the seller's company profile and products, there should be clear steps on how the seller can access data it has shared with the eCommerce company.

vi. Spell out the procedures for dealing with requests for data deletion or return of data to the data originator.

vii. How all data sharing activities will be recorded and tracked should also be noted.

c) In a data sharing environment that involves multiple stakeholders in the eCommerce value chain, the agreement should make clear the relevant single point of contact for data originators to reach out to in case of queries or if they want to exercise their rights as data originators. As an example, if an eCommerce company goes into a data sharing agreement with marketplace sellers, logistics providers, and payment partners and is storing data from these partnerships, the eCommerce company should specify the personnel responsible such as a data protection officer who can help manage data-related queries. Similarly, an eCommerce platform user should be able to reach out to a data protection officer for any concerns or grievances regarding the user's data. This contact person can be located at the privacy policy page of the eCommerce website.

d) A data provider must ensure that access to any data obtained from a data originator is properly audited and any changes made to the data is traceable. As an example, if an eCommerce company has provided access to a customer's data to a logistics provider, this event must be logged and can be made available to the customer if required.

e) Data retention period should also be clearly mentioned in the agreement. While a period of seven years is recommended as a general retention period, eCommerce stakeholders can validate and determine the periods in their agreements taking into account factors such as volume and type of data involved, cost for retention, and return on investment, among others.

f) Any data that will be stored or shared cross-border by a data user must be explicitly stated in the agreement. The relevant data privacy laws and regulations that become applicable for data stored or shared cross-border must be explicitly made known to the data originator. As an example, if an eCommerce company engages the services of a cloud service provider whose datacentre is in a different country, then the eCommerce company must ensure that the agreement will call out the regulatory implications of the data being stored in that particular country. This information can also be stated in the privacy policy page of the eCommerce website.

g) eCommerce companies must ensure that consent is obtained from parents or guardians, should there be a need to collect data that contains information of minors. In the event that this information is not required, eCommerce websites should clearly mention that data in relation to minors will not be collected.

h) eCommerce companies must ensure that the eCommerce website clearly states provision for intellectual property rights to be protected.

i) eCommerce companies must ensure that their privacy policy page lists down the relevant policies that their organisation adheres to, such as the Personal Data Protection Act 2010 (PDPA) and the like.

Relevant Existing Acts Referred

a) The PDPA, in covering rights for personal data, provides the following provisions for data sharing:

    i. A data user should not process personal data unless consent has been provided by the data owner.

    ii. A data user will have to provide a formal written notice to a data owner should they wish to process personal data on behalf of the data owner, which includes details such as description of the personal data, purpose of collection and sharing of the personal data, information on the source of the personal data, rights of the data owner to be able to request access and to correct the personal data, the stakeholders that the data user will be sharing the personal data with, and the boundaries of the sharing of this personal data.

    iii. A data owner should also be promptly notified by the data user whenever the data user first collects personal data, uses the personal data for reasons other than what was agreed upon, or discloses the personal data to a third-party.

    iv. A data owner will also have the authority to correct personal data whenever it is inaccurate or incomplete, outdated, or misleading, and withdraw consent to process personal data.

b) The Computer Crimes Act (1997), provides the following provisions when it comes to data privacy:

    i. It is a punishable offence if unauthorised access to any computer material is performed.

    ii. It is a punishable offence if unauthorised modification of computer material is performed.

    iii. It is a punishable offence if unauthorised access to any computer material is performed with the intention of further utilising the material obtained.

c) The Communications and Multimedia Act 1998 (CMA) mentions that interception and disclosure of communications or attempts to intercept and disclose to any other individual the contents of any communications are forbidden.

d) The Consumer Protection Act 1999 (CPA) ensures consumer protection in that the personal data of a buyer cannot be disclosed or circulated to third parties unless the buyer has been informed regarding the purpose of sharing the data, and with written consent from the buyer.

2.3. Data Security

a) To protect data that is being collected and shared, data users must ensure that these data are being processed securely, with appropriate organisational and technical measures in place. The security measures must be appropriate to the nature, scope, context, and purpose of the processing, as well as address the risks posed to the rights and freedoms of the data originator.

b) The data sharing agreement should contain the following elements for data security:

   i. Clarity and details on the sensitivity levels of data that will be collected and shared.

   ii. Agreed-upon steps of security standards to be practiced by the data user.

   iii. The allowable exceptions in case there will be unavoidable differences in the standards of security, and the steps in managing these by the data originator and data users. For example, if an eCommerce company and a logistics partner have differing data security practices, then the differences should be listed as exceptions if an agreement is reached between both parties.

c) A communication process must be put in place to ensure that a data originator is promptly informed in the event of any breach or tampering of their data. The data originator should be informed about the impact of the breach, the steps being taken to rectify the impact of the breach, and how such instances will be avoided in the future. This communication process should also be clearly mentioned in the privacy policy page on eCommerce websites. As an example, if an eCommerce company suffers data breach in which customers' email addresses have been made available on the internet, the eCommerce company must ensure that its communication process is triggered per the stipulated timeframe and sent out to all affected customers. Details around what other information apart from email addresses have been leaked should be made known, including the time and method of breach and the recovery period.

d) Data users who store data from data originators must implement a data back-up and recovery regimen that is appropriate for the scale, sensitivity, and timelines of the data stored.

e) Stored data must be encrypted and there should be an access control mechanism at each data storage device or software, whereby proper registration and credentials are needed to access specific fields of data. Where possible and depending on the scale and criticality of the data, it is recommended to engage with reputable datacentres for the secure storage of data.

Relevant Existing Acts Referred

a) According to the PDPA, a data user is required to take practical measures to protect personal data from misuse, loss, modification, accidental or unauthorised access or disclosure, destruction, or alteration. Security measures must be taken and applied to any equipment that stores personal data to ensure the integrity, reliability, and competence of personnel that has access to the personal data. There should be proper measures to ensure the secure transfer of personal data.

    i. The PDPA also requires that data processed for any purpose should not kept longer than necessary for the fulfilment of that purpose and it is the duty of the data user to ensure that all personal data is destroyed or permanently deleted if it is no longer required.

b) The Companies Act (1965) mentions that every company shall retain records for seven years after the completion of the transactions or operations to which they respectively relate. These records include:

    i. Accounting records.

    ii. Other records that will adequately explain the transactions and financial position of the company.

c) The Computer Crimes Act (1997) mentions that an individual who has unauthorised access to data held in any computer shall be liable to imprisonment for a duration of not more than five years, or a fine of not more than fifty-thousand ringgit, or both.

d) The Communications and Multimedia Act 1998 (CMA) has the following provisions when it comes to data security:

    i. Any unauthorised access of data via network means without prior approval is subject to fine and imprisonment terms.

    ii. Any unauthorized transmission of data via network means without prior approval is subject to fine and imprisonment terms.

Section 3: Case Studies

3.1. Sharing Customer Data with a Logistics Partner

An eCommerce company shares its customer's name, contact data, purchase content, and value to a logistics partner. A contract should be agreed upon by the eCommerce company and the logistic partner to ensure that data shared are not misused or leaked to external parties. This should be applicable to both local shipments and cross-border shipments. The data that the logistics company analyses should not be tied to the eCommerce company's customer's personal data. The contract should clearly state the specific usage of data and categorise each data collected, stating which data will be shared or analysed and for what purpose. The logistics company should have proper security measures in place to protect this data, audit trails, and have multifactor authentication for access to data. Awareness sessions, trainings, and workshops on data sharing, and data privacy should be held regularly so that all personnel are well-equipped in handling data.

Having such security measures in place is essential because by having access to the customer's personal data, such as an individual's phone number, external parties can already easily identify the individual's full name per their identity card. This is due to some eWallet payment applications that allow the transfer of money using an individual's phone number. Additionally, as best practice, personal data should be removed from parcel labels to protect customer's personal information. Besides that, purchase history, purchase content, and purchase value are also sensitive information tied to an individual's identity data, so such data must be protected and properly secured when shared with logistic partners. This should also apply to instances when a logistic partner outsources orders to third-party courier services.

3.2. Sharing Customer Data with a Payment Partner

An eCommerce company partners with a payment gateway provider. The eCommerce company does not store any customer information on its website, as the customer's private and sensitive payment information are stored with the payment gateway provider. The eCommerce company will only have access to certain information such as customer's name, name of the bank, and the last four digits of the payment card used. This is so that eCommerce companies can check on a transaction or cancel an order. The payment gateway provider should be meet the standards of Payment Card Industry Data Security Standard (PCI DSS).

If an eCommerce company does not partner with a third-party payment gateway provider, the eCommerce company should apply for a PCI DSS certificate. This is to prevent customer credit card information data from being compromised, and to ensure adherence to PDPA whereby practical and security measures should be taken to protect personal data from unauthorised access.

3.3. Rights of Individual

An eCommerce platform user wants to remove their data. However, they do not know how to do so, hence the user visits the privacy policy page, which lists the steps on data deletion.

Individuals whose data has been collected by eCommerce companies and their partners should have the option to unsubscribe to the sharing of their personal data. The option to delete their data should be made available to them either via email, mail, live chat, or a checkbox option in the settings page. Deletion of data should be made by the ecommerce company as well as its partners with which the data was shared. Nevertheless, order-related data does not need to be deleted as this data is required for company audit purposes. Similarly, brand vendors and marketplace sellers should have this option to remove their data stored with the eCommerce company should they wish to.

3.4. Protection of Minors

An eCommerce company offers printing services that may consist of images for children and minors. The data shared by customers are stored securely and strictly used for the purpose of the service, meaning data is not shared to any external party. However, in instances where this service was provided as part of a “giveaway contest”, contestants would have consented to the use of image shared by them, to external parties as part of the terms and conditions of participating in the contest.