NTT DATA Payment Services Sdn. Bhd.
(formerly known as GHL Systems Sdn. Bhd.)
Group Personal Data Protection Policy

NTT DATA Payment Services Sdn. Bhd.
C-G-15, Block C, Jalan Dataran SD1,
Dataran SD, PJU 9, Bandar Sri Damansara,
52200 Kuala Lumpur, Malaysia.

www.nttdatapay.com

VERSION CONTROL

Version	Approval Date	Prepared by	Approved by
1.0	18/10/2023	Group Legal, Compliance & Sustainability	Group CEO
2.0	19/11/2025	Group Legal, Compliance & Sustainability	Board of Directors

COPYRIGHT AND OWNERSHIP

This Group Personal Data Protection Policy is issued by Group Legal, Compliance & Sustainability.

CONTENTS

1. INTRODUCTION

1.1. NTT DATA Payment Services Sdn. Bhd., together with all our related corporations as defined under the Companies Act 2016, and any other entities within the NTT DATA Group for which NTT DATA Payment Services Sdn. Bhd. provides management oversight and strategic direction as the regional headquarters, now and in the future (collectively, "**NTT DATA Payment Services Group**", "**we**", "**us**", or "**our**") are committed in complying with the Personal Data Protection Act 2010 ("**PDPA**") and any other applicable data protection laws. As a subsidiary of NTT DATA Japan Corporation and a part of the NTT DATA Group, we are dedicated to upholding the principles and standards of the NTT DATA Group Data Protection Policy. NTT DATA Group refers to NTT DATA Group Corporation and its consolidated subsidiaries.

1.2. We at NTT DATA Payment Services Group respect the privacy of individuals in respect of their personal data, as reflected in this Group Personal Data Protection Policy ("**Policy**"). The purpose of this Policy is to ensure compliance that all employees, contractors, part-timers, temporary staff, volunteers, secondees and officers of the NTT DATA Payment Services Group (collectively, "**Staff**") understand their responsibilities and obligations under the PDPA.

1.3. All Staff should refer to this Policy when dealing with personal data, as this Policy describes:

- the types of personal data collected by the NTT DATA Payment Services Group, the ways and purposes personal data is collected and the parties to whom personal data is disclosed to; and
- the responsibilities of the Staff in relation to the handling and processing of personal data in connection with their role within the NTT DATA Payment Services Group.

1.4. The PDPA establishes an overarching regime for the protection of personal data and seeks to ensure that organisations comply with a baseline standard of protection and accountability for personal data of individuals. The PDPA will operate concurrently with other legislative and regulatory frameworks which may be applicable to the NTT DATA Payment Services Group. This means that where personal data is processed in or in connection with other jurisdictions outside of Malaysia, the relevant data protection law of such jurisdiction (separate from the PDPA) may apply concurrently with the PDPA. If this Policy is accessed or applied outside of Malaysia where another data protection framework (aside from the PDPA) is applicable, then such data protection framework (in addition to the PDPA) must also be complied with.

1.5. Staff must read, understand and comply with all provisions of this Policy. Staff must only collect, use and disclose personal data in accordance with this Policy, unless otherwise instructed by your supervisor in writing.

1.6. This Policy may be updated from time to time.

2. COLLECTION OF PERSONAL DATA

2.1. For the purposes of this Policy, "personal data" refers to any data or information about you, which can relate to a specific identifiable individual, whether from the data itself or from other information which is reasonably available to NTT DATA Payment Services Group or the Staff. Examples of personal data

include:

2.1.1. names, identification or passport number, telephone number, address, email address, photographs or video recordings and biometric data;

2.1.2. information relating to an individual's use of websites and services, including cookies, IP addresses, subscription account details and membership details;

2.1.3. employment history, education background, and income levels;

2.1.4. payment related information, such as bank account or credit card information and credit history; and

2.1.5. sensitive personal data or information relating to individuals, as defined under the PDPA.

2.2. The NTT DATA Payment Services Group collects personal data through various means, including but not limited to any online communication from any individuals, registration for any products or services, market surveys, promotions, application for any work position or scholarship and any other form of direct or indirect provision of personal data from the individual for any reason. We may monitor or record phone calls and customer-facing interactions for quality assurance, employee training and performance evaluation, and identity verification, receiving feedback, responding to your queries, requests and complaints and other related purposes.

3. USE AND DISCLOSURE OF PERSONAL DATA

3.1. In general, NTT DATA Payment Services Group can only collect, use or disclose the personal data of an individual with the individual's consent, and for a reasonable purpose which the organisation has made known to the individual. NTT DATA Payment Services Group is also required to provide individuals access to their personal data and consider requests to correct the personal data it holds or controls. Specific key obligations under the PDPA are set out below:

3.1.1. **Consent principle**: The consent of the relevant individual must be obtained before any collection, use or disclosure of their personal data, unless exceptions apply. Organisations must allow the withdrawal of consent which has been given or deemed to be given.

3.1.2. **Notice principle**: Individuals must be notified of the purposes for the collection, use, disclosure or processing of their personal data, prior to such collection, use, disclosure or processing.

3.1.3. **Disclosure principle**: Personal data must not be disclosed to any third party unless the consent of the individual has been obtained.

3.1.4. **Security principle**: Organisations must implement reasonable security arrangements for personal data, including to prevent unauthorised access, collection, use, disclosure, copying, modification or disposal, or similar risks, and the loss of any storage medium or device on which personal data are stored.

3.1.5. **Retention principle**: Organisations must not keep personal data for longer than it is necessary to fulfil: (i) the purposes for which it was collected; or (ii) a legal or business purpose.

3.1.6. **Data integrity principle**: Organisations must take reasonable steps to ensure that all personal data processed is accurate, complete, not misleading and kept up-to-date by having regard to the purpose, including any directly related purpose, for which the personal data was collected and further processed.

3.1.7. **Access principle:** When requested, organisations must: (i) provide individuals with their personal data in the possession or under the control of the organisation and information about the ways in which the personal data may have been used or disclosed during the past year; and (ii) correct an error or omission in an individual's personal data that is in the possession or under the control of the organisation.

3.1.8. **Data breach notification obligation**: Organisations must take certain actions where they have reason to believe that a data breach affecting personal data in their possession or under their control has occurred.

3.2. We require organisations outside of NTT DATA Group which handle or obtain personal data as service providers to us acknowledge the confidentiality of the personal data, undertake to respect any individual's right to privacy and comply with the PDPA and any other applicable data protection laws. As a requirement under these laws, we may be required to have specific agreements in place with such third parties to regulate and safeguard your data protection rights. We also require that these organisations use this information only for our purposes and follow our directions with respect to this information.

4. TRANSFER OF PERSONAL DATA

4.1. NTT DATA Payment Services Group may transfer personal data to places outside of Malaysia if the consent of the individual has been obtained or if a specific exception under the PDPA is applicable. This requirement applies to transfers of personal data to any affiliate or related entity of NTT DATA Payment Services Group located outside of Malaysia.

4.2. Before transferring personal data overseas, NTT DATA Payment Services Group must conduct due diligence to ascertain that the receiving organisation provides a comparable level of protection, considering amongst other factors, the nature of the personal data, the reputation of the receiving organisation and the laws of the country.

5. RETENTION OF PERSONAL DATA

5.1. NTT DATA Payment Services Group shall cease to retain documents containing personal data, or remove the means by which the personal data can be associated with particular individuals, as soon as it is reasonable to assume that:

5.1.1. the purpose for which that personal data was collected is no longer being served by retention of the personal data; and

5.1.2. retention is no longer necessary for legal or business purposes.

5.2. NTT DATA Payment Services Group may retain personal data for as long as it is necessary for the purposes for which it has been collected, up to seven (7) years, unless otherwise permitted by

applicable law or in order to defend legal claims.

6. RIGHTS AND CHOICES OF DATA SUBJECTS

6.1. Please note that individuals have the following rights:

6.1.1. obtaining confirmation in respect of the processing of their personal data and to request a copy of their information;

6.1.2. rectification of personal data to ensure the personal data is accurate and up-to-date;

6.1.3. the right to receive personal data in a structured manner, where the processing of the personal data is carried out by automated means;

6.1.4. in certain circumstances, request to delete or restrict the processing of personal data;

6.1.5. object the processing of personal data in certain circumstances, unless there are compelling legitimate grounds to continue processing or where it is necessary for legal reasons;

6.1.6. prevent any processing of personal data that is causing or is likely to cause unwarranted and substantial damage or distress to the data subject or any individual;

6.1.7. be informed about any use of the personal data; and

6.1.8. to lodge a complaint about the way in which the personal data is being used to a supervisory authority.

7. DATA BREACH MANAGEMENT

7.1. A personal data breach broadly refers to any event or incident that leads or is likely to lead to the breach, loss, misuse, or unauthorised access of personal data.

7.2. Personal data breaches may happen for different reasons, including as a result of malicious activities (such as computer hacking or data theft), human errors and IT system errors. We require our employees to be alert and be aware of the risks of data breaches when handling any personal data.

7.3. In case an employee suspects or becomes aware that a personal data breach may have or has occurred, such employee must immediately notify the relevant Data Protection Officer (based on the jurisdiction where the employee is based) as directed under paragraph 9 below and Group Operational Risk, in line with the Incident Reporting Standard of Procedure, within 24 hours. The notification should at least contain the following information:

7.3.1. the date and time of the incident, and when it was discovered;

7.3.2. a description of the incident; and

7.3.3. any other information as may be required by the Data Protection Officer and/or the Group Operational Risk.

7.4. The speed of reporting the incident is critical and crucial. Further, all data breach information must be kept strictly confidential and must not be disclosed to any party unless otherwise instructed by the Data Protection Officer.

7.5. In managing personal data breaches, we will consider the context and the circumstances of the incident, and seek professional external assistance if required. If a personal data breach is notifiable to the relevant data protection regulators (e.g. the Personal Data Protection Commissioner ("PDPC") in Malaysia) or the affected individuals, we are committed in complying with the requirement to notify the incidents to the relevant parties in a timely manner and with appropriate modes of notification.

7.6. The Data Protection Officer is responsible for preparing and submitting notifications to data protection regulators. Where affected individuals must be notified, the relevant business unit (e.g. the operational team or relationship manager) will prepare the notice. The Data Protection Officer and Group Operational Risk will review and approve the notice before the business unit sends it out. The notification will outline the breach, associated risks, and recommended mitigation steps.

7.7. For breaches occurring in Malaysia, the following timeframes apply:

7.7.1. Data protection regulators: Notification to the PDPC must be submitted within 72 hours from when the breach occurred.

7.7.2. Affected individuals: Notification must be issued within 7 days from when the PDPC is notified.

8. MANAGEMENT AND SECURITY

All reasonable efforts and practical steps are made to ensure that any Personal Data held is kept up to date and is protected against any loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction. We will, amongst other things:

8.1.1. store the personal data collected in an appropriate location, which is unexposed and safe from physical or natural threats;

8.1.2. provide a user ID and password for authorised employees to access personal data and terminate the user ID and password immediately if the employee is no longer authorised to access the personal data;

8.1.3. keep a record of all authorised employees involved in the processing of personal data and ensure that the authorised employees protect the confidentiality of the personal data;

8.1.4. terminate an employee's access rights to personal data after his/her resignation or termination;

8.1.5. control and limit employee's access to our personal data systems;

8.1.6. monitor and control any entry to or exit of our data site, including but not limited to, providing a closed-circuit camera or a 24-hour security monitoring;

8.1.7. update the necessary recovery system and anti-virus software on our personal data systems and safeguard the systems from any malware threats;

8.1.8. prohibit the transfer of personal data through removable media device and cloud computing service without the written permission of an authorised officer;

8.1.9. record any transfer of personal data through removable media device and cloud computing service;

8.1.10. comply with personal data protection principles in Malaysia or any other applicable data protection laws of other jurisdictions in respect of any personal data transfer via cloud computing service; and

8.1.11. maintain a proper record of access to personal data.

8.2. If we appoint a third-party data processor to process personal data on behalf of the NTT DATA Payment Services Group, we will bind the third-party data processor with a data processing agreement to ensure the safety of personal data from any loss, misuse, modification, unauthorised access, and disclosure.

8.3. We also take practical steps to protect the personal data it collects and processes non-electronically or in hard copy format from any loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction. We will, amongst other things:

8.3.1. keep a record of all authorised employees involved in the processing of personal data and ensure that the authorised employees protect the confidentiality of the personal data;

8.3.2. terminate an employee's access rights to personal data after his/her resignation or termination;

8.3.3. control and limit employee's access to our personal data system;

8.3.4. store such personal data;

(a) in an orderly manner, for example, in files;

(b) in a locked place, where all the related keys are kept and stored in a safe place and recorded; and

(c) in an appropriate location which is unexposed and safe from physical or natural threats;

8.3.5. maintain a record of access to personal data;

8.3.6. maintain a record of personal data transferred conventionally, e.g. via mail, deliver and fax;

8.3.7. ensure that all used papers, printed documents, or other documents with personal data are thoroughly and efficiently destroyed by using shredding machine or other appropriate methods; and

8.3.8. conduct training and/or awareness programmes to all employees, if necessary, on the responsibility to protect personal data.

8.4. In addition to the above, we have also appointed Data Protection Officers to oversee our management of personal data in accordance with this Policy and the PDPA, including any other applicable data

protections law. Our employees must handle all personal data confidentially, and we regard any breaches of any applicable data protection laws very seriously.

9. CONTACT DETAILS

9.1. If you have any questions or queries relating to the processing of any personal data, or if you are unsure about any internal data practices of the NTT DATA Payment Services Group, please contact the Group Legal, Compliance & Sustainability department at grouplegal@ghl.com or the relevant Data Protection Officer. For more information about the Data Protection Officer, please refer to our Privacy Notice at https://www.nttdatapay.com/en/privacy-notice.

10. REVIEW OF THIS POLICY

10.1. This Policy will be reviewed from time to time, taking into account changes in laws and regulations, changes to NTT DATA Payment Services Group's internal operations and practices, and the changing business environment. You should ensure that you are referring to the latest version of this Policy at all times.