NTT DATA Payment Services Sdn. Bhd.

(formerly known as GHL Systems Sdn. Bhd.)

Group Management of Customer Information and Permitted Disclosures (“MCIPD”) 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	25/08/2022	Group Legal, Compliance & Sustainability	Board of Directors
2.0	27/04/2024	Group Legal, Compliance & Sustainability	Board of Directors
3.0	30/07/2025	Group Legal, Compliance & Sustainability	Board of Directors

COPYRIGHT AND OWNERSHIP

This Group Management of Customer Information and Permitted Disclosures ("MCIPD") Policy is issued by Group Legal, Compliance & Sustainability.

CONTENTS

1. INTRODUCTION

The Group is committed to conduct business in accordance with the highest ethical standards and in full compliance with the laws on Personal Data Protection and Data Privacy on each country in which we have presence in, which governs the processing of personal data for commercial transactions.

The Group handles and shares a significant amount of customer information in the course of providing financial services and products in particular to the Group's Outsourced Service Provider and employees. Proper handling of customer information is critical in establishing public trust and confidence and mitigating reputational damage to the Group. Therefore, it is critical for the Group to protect the customer information from theft, loss, misuse, or unauthorized access, modification or disclosure through any means, including verbal or written disclosure.

2. OBJECTIVES

The objectives of this Group Management of Customer Information and Permitted Disclosures ("MCIPD") Policy ("Policy") are as follows:

a) to safeguard customer information against theft, loss, misuse, or unauthorized access, modification, or disclosure by any means, including verbal or written disclosure;

b) to reaffirm the Group's commitment to complying with all applicable legal and regulatory disclosure obligations; and

c) to ensure that all parties covered by the Policy are aware of their responsibility to protect customer information confidentiality.

3. APPLICATION AND DEFINITION

3.1 APPLICATION

This Policy applies to all directors, Senior Management, employees, and outsourced service providers of the Group, across all business and operations of the Company.

3.2 DEFINITION

TERM	DEFINITION
Company	NTT DATA Payment Services Sdn Bhd

Customer	Any person/s who use/s, has used or may be intending to use, any financial services or product including- (a) representative of the customer (such as the parents of a minor and authorized representative); and (b) a person who has entered or intend to enter into arrangement with The Company (such as a guarantor or third party security provider) on account of or for the benefit of a customer.
Customer Information	Any information relating to the affairs or, in particular, the account, of any particular customer of the Company in whatever form including in the form of a record, book, register, correspondence, other document or material;
Disclosure	Disclosure by transmission, transfer, dissemination or by any other means, including verbally or in writing, by which customer information is made available by any person who has access to such customer information to another person;
Group	NTT DATA Payment Services Sdn Bhd, its 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, with each such company being a member of the NTT DATA Payment Services Group of Companies;
NTT DATA Group	NTT DATA Group Corporation and its consolidated subsidiaries
Outsourcing Arrangement	Arrangement in which an outsourced service provider performs an activity on behalf of the Company on a continuing basis, where the activity is normally or could be undertaken by the company;
Outsourced Service Provider (OSP)	Entity, including an affiliate, providing services to the Company under an outsourcing arrangement and includes all sub-contractor(s);
PDP	Personal Data Protection and/or Data Protection Laws of the relevant Countries and/or General Data Protection Regulation (GDPR) subject always the PDP laws of that particular Country shall prevails in the event of any conflicts or contradictions;
PCIDSS	Payment Card Industry Data Security Standard as certified by the PCI Security Standard Council;
Representatives and Agents	Any individual or firm or companies acting on behalf of the Company;
Senior Management	Group Chief Executive Officer, Country Chief Executive Officers Group Heads of Departments and Heads of Departments;

Staffs	All persons employed by the Company, including temporary or contract staff, consultants, officers on attachment from an affiliate or internship staff.

4.0 INFORMATION CONFIDENTIALITY

4.1 All staffs and OSPs are required to handle customer information and company profile in accordance with the PDP laws of the particular country in line with this Policy.

4.2 Staffs shall not discuss or disclose customer information with any other NTT DATA Payment Services staffs who are not related to their Departments except insofar as it is necessary for work-related purposes or any other third party without authorization from the Senior Management.

4.3 All Staffs are bound by their Letter of Offer for Employment which includes but not limited to the Confidentiality Clause that includes complying with the PDP laws.

4.4 All OSPs shall sign a confidentiality or a non-disclosure agreement ("NDA") integrated within their Contract of Engagement or Letter of Appointment with the Company and/or its affiliates. All information given or developed or obtained or supplied by or on behalf of the Company shall remain the sole property of the Company and shall in no way be sold, copied or used in whatsoever manner without the express written consent of the Company.

4.5 the Company shall at all times ensures that appropriate controls are in place and are effective in safeguarding the security, confidentiality and integrity of any information shared with the service provider. In meeting this requirement, all staffs must ensure that: -

a) all information disclosed to the OSP is limited to the extent necessary to provide the contracted service and only on a need-to-know basis;
b) all information shared with the OSP is used only to the extent necessary to perform the obligations under Contract of Engagement or Letter of Appointment in accordance with the outsourcing arrangement;
c) all customer information obtained by the OSP in accordance with the purpose as stated in their Contract of Engagement or Letter of Appointment in accordance with the outsourcing arrangement on behalf of the Company shall be belong to the Company solely;
d) OSP are not to divulge any of the said customer information unless the said customer information is no longer of use to the Company in which event the OSP must destroy or erase the said customer information from their date base immediately;

e) the OSP must store all the customer information in a server or data room or any similar storage system which must be PCIDSS certified or its equivalent as and when required by law of that particular country;

f) the OSP must also ensure all physical copies of the customer information must be stored in a highly secured area and manner which are not accessible by any third party;

g) all locations where customer information is processed or stored, including back-up locations, must be made known to the Company at all times; and

h) where the OSP is located or performs the outsourced activity, outside of the Company office in the country in which the office is operated, the OSP must be subjected to the Data Protection laws and standards that are at the very least equivalent or of higher standards than the PDP laws of the Company Office which the OSP is contracted to.

5.0 ACCESS CONTROL MEASURES

5.1 the Company may engage other companies, service providers or individuals or any third party to perform functions on its behalf, and consequently may provide access or disclose customer information to the third parties such as those listed below (list of which is not exhaustive) (“permitted disclosures”):

a) information technology service providers;

b) data entry service providers;

c) regulatory and governmental authorities in order to comply with statutory and government requirements; and

d) potential buyer of transferee in the event of any re-organization or disposal of the Company’ business or any part thereof.

5.2 The the Company’ Board of Directors (“Board”) is ultimately responsible for ensuring that this Policy is effectively implemented and that the permitted disclosure requirements are met.

5.3 This Policy shall be agreed and approved by the Board to safeguard the Company’ customer information against theft, loss, misuse or unauthorized access, modification or disclosure by whatsoever means.

5.4 The Board of Directors shall be held accountable and responsible for developing and implementing procedures, including effective systems and controls, to protect customer information.

5.5 the Company has appointed a Group Chief Technology Officer who oversees all data including the customer information that are stored in the data centres and also a Group Chief Risk Officer who oversees all the customer information for risk assessment purposes.

5.6 In line with the aforesaid, each the Company Subsidiaries in each country must develop and implement all control measures, escalation (if any) and permitted disclosures requirements of each relevant departments and forward them to the Group Risk Department and the Group Legal, Compliance and Sustainability Department.

6.0 ASSESSMENT AND AUDIT OF OUTSOURCED SERVICE PROVIDER

6.1 Conducting a comprehensive and robust due diligence process is necessary for the Company to make an informed selection of OSPs in relation to the risks associated with the outsourcing arrangement. This is to ensure that customer information is handled with care in order to protect the customer's privacy.

6.2 the Company shall conduct appropriate due diligence of an OSP at the point of considering all new arrangements and renewing or renegotiating existing arrangements. The scope and depth of the due diligence process will be commensurate with the materiality of the outsourced activity.

The due diligence process covers, at a minimum as follows:

a) capacity, capability, financial strength and business reputation;
b) risk management and internal control capabilities including physical and IT security controls, and business continuity management;
c) the location of the outsourced activity, including primary and back-up sites; and
d) reliance on sub-contractors, if any, in particular where the sub-contracting adds further complexity to the operational chains of the outsourcing arrangement.

6.3 In performing due diligence on the OSPs, the Company shall ensure an objective assessment of the OSP's ability to perform the outsourced activity and the outcomes of the due diligence process are well-documented and escalated to the Board, where relevant, in line with the outsourcing risk management framework of the Company.

6.4 the Company must perform an audit or an independent review by its Internal Audit at least once every two (2) years on the OSPs to ensure the customer information is protected from theft, loss, misuse or unauthorized access, modification or disclosure by whatsoever means.

7.0 OUTSOURCED SERVICE PROVIDER AGREEMENT

7.1 All outsourcing arrangement must be governed by a Contract of Engagement or Letter of Appointment in accordance with the outsource arrangement and Contract of Engagement or Letter of Appointment must, at a minimum, provide for the following:

a) duration of the arrangement with date of commencement and expiry or renewal date;

b) responsibilities of the OSP with well-defined and measurable risk and performance standards in relation to the outsourced activity;

c) controls to ensure the security of any information shared with the OSP at all times, covering at a minimum: -

i. responsibilities of the outsource service provider with respect to information security;

ii. scope of information subject to security requirements;

iii. provisions to compensate the the Company for any losses and corresponding liability obligations arising from a security breach attributable to the service provider;

iv. notification requirements in the event of a security breach; and

v. applicable jurisdictional laws.

8.0 INTERNAL DATA ACCESS RESPONSIBILITY

8.1 the Company shall at all times ensure that all information is secured and protected from any unauthorized access.

8.2 It is the utmost priority for the Company to ensure that all staffs are responsible in managing the customer information.

8.3 Therefore, all staffs are provided with training pursuant to the PDP laws to ensure proper handling of all the customer information and company profile to avoid any leakage of information to a third party or data breach incident.

8.4 To minimize unintentional disclosure or misuse of customer information, all staffs are responsible to adopt practices to maintain confidentiality at all times, including outside of the Company' premise, which include but not limited to the following:

a) Documents and files containing customer information should be kept in a safe place with restricted access or within the the Company' secured IT system with accessibility

restricted only to selected individuals who "need to know" in the necessary course of business. Code names should be used, where necessary;

b) Customer information should not be discussed in places where the discussion may be overheard by persons not authorized to have the information, including but not limited to, elevators, hallways, restaurants, bars, restrooms, airplanes or taxis. Should customer information be discussed on wireless devices in public areas, arising from urgency or necessity, caution must be exercised by the individuals;

c) Customer information should not be read or displayed in public places or discarded where they can be retrieved;

d) Transmission of documents by fax, email or any other electronic devices or means should be made only where it is reasonable to assume that transmission can be made and received under secured conditions;

e) Documents containing customer information should be promptly removed from conference rooms and work areas after meetings have concluded and extra copies of the documents should be destroyed;

f) Circulation of documents containing customer information must be, where appropriate, protected through secured means including sealing, authentication or password protection; and

g) All visitors should be accompanied by staffs so that they are not left unaccompanied in offices or sites containing customer information.

8.5 As the Company is a company that deals with cashless and online payments business, there are not many documents that are kept physical but should there be, the following are the steps taken to ensure that information are properly managed, handled or transported with regard to those documents containing the customer information:

a) All documents that needs to be transported out from the office must be approved by the respective Senior Management of the Department;

b) To synchronise on the said process of the aforesaid approval, an approval form in the format as contain in Appendix A herein must be executed and be kept by the relevant department as so determined by the respective Senior Management of the Department; and

c) The above shall be audited by the Internal Audit in accordance with Paragraph 6.4 herein.

9.0 MANAGING CUSTOMER INFORMATION BREACHES

9.1 A potential breach of customer information may be identified through complaints from customers or internal alerts by employees.

9.2 Any breach of customer information must be declared and escalated to the respective Head of Department ("HOD") or his/ her direct superior for further action. The HOD shall notify the breach to the Group Chief Technology Officer, the Group Risk Chief Officer and to the Group Chief Executive Officer and thereafter to the Board with an Incident Report detailing what happened and what action will be or has been taken to mitigate or close the said breach.

9.3 The reporting shall be made as and when the conflict arises, and shall be made at the earliest opportunity i.e. as soon as the employee becomes aware of the breach.

9.4 With the advice from the Group Chief Technology Officer and/or the Group Chief Risk Officer, appropriate mitigating actions shall be taken to contain the breaches including but not limited to the following:-

a) the Company' systems lockdown;

b) Changing access control credentials; and/or

c) Preserving firewall settings, firewall logs, system logs, and security logs.

9.5 IT Department and Risk Department will be responsible for the reporting of the breach of customer information to the Group CEO and/or the Board. Upon receiving the report, IT Department and Risk Department shall assess the impact of the breach, investigate, and ensure remedial actions are put in place to prevent future recurrence within three (3) months from the date of which the breach was detected.

9.6 Once the investigation has been concluded, a full investigation report shall be reported to the Board and subsequently submitted by IT Department to the following:-

Director
Payment Services Oversight Department
Bank Negara Malaysia
Jalan Dato' Onn
50480 Kuala Lumpur

10.0 DISPOSAL OF CUSTOMER INFORMATION

10.1 Any customer personal information that is deem not required must be securely disposed of which includes any physical and/or digital records of the customer personal information through the following ways:

a) Physical documents – cross-cut shredding or incinerating;

b) Digital documents – deletion, degaussing, reformatting or destruction of the device used for storage; and
c) Any other methods that is approved in writing by the respective HODs.

10.2 Prior to any disposal of customer information, all staffs and OSPs must ensure the following:

a) the information is no longer required and does not need to be archived for any business or legal reasons; and
b) an approval has been obtained from the relevant HODs or his/ her direct superior.

A record of such disposal shall be kept for operational and compliance purposes by the respective departments for at least seven (7) years.

10.2 For any transportation of customer information outside of any of the office premises for the purpose of destruction by a third party, the information shall be shredded or stored sealed in bags with tamper proof fastener or stored in locked containers before it is collected by the third party. Once the destruction is complete, the third party shall provide the Company with a written certification of such destruction within a reasonable time and the said certification shall be kept by the relevant Departments for audit purposes. The responsibility of ensuring the above is carried out smoothly shall be the relevant HODs.

9.0 POLICY COMPLIANCE

The Group expects all employees to fully comply with this Policy. This policy, as stated above, shall be subjected to audit by the Internal Audit to review the effectiveness of its implementation at least once every two (2) years.

APPENDIX A

Transportation of Physical Document Form

Employee/Sender Name :	**Employee no. :**
Name of Company/Subsidiary :	**Designation/Department :**
Name of Reporting Manager :	**Email Address :**

Details of Document

Description of Document:	
Origin:	**Employee/Sender:** **……..** **Name:** **Designation:** **Date:**
Destination:	**Receiver:** **……..** **Name:** **Designation:** **Date:**
Approved by HOD: **…….** **Name:** **Designation:** **Date:**	