NTT DATA
PAYMENT SERVICES

Information type: Confidential (related parties only)
Company: NTT DATA GROUP

Information owner: Global Governance HQ

NTT DATA Group
Data Protection Policy

Contents

1. Introduction

NTT DATA Group aims to grow its business by providing services to customers and society through the development of diverse businesses, such as systems development, IT consulting, cloud computing services, and data center services, in many countries and regions worldwide.

As we promote our business using information technology, we process a variety of data, including personal data, that must be processed in an appropriate manner. We respect individuals' privacy, and protect the personal data we process. We also balance our need to process personal data in connection with our activities with the legal requirements to protect it.

In recent years, data subjects' privacy rights have been emphasized on a global scale, and data protection laws and regulations have been established or strengthened in various countries and regions, including the General Data Protection Regulation of the European Union ("GDPR"), the California Consumer Privacy Act ("CCPA"), the Personal Information Protection Law of China ("PIPL"), and the Act on the Protection of Personal Information of Japan ("APPI").

The processing of personal data takes place in a much larger, ever-evolving context, which includes legislation in several countries that addresses other aspects of and challenges to responsible (personal) data governance, from cybersecurity to the use of Artificial Intelligence ("AI"), all of which have demanded appropriate responses to data protection. We need to be aware of trends in these areas as they relate to data protection, and of our responses to laws, regulations, and the Group's company rules.

Furthermore, as business collaboration among the Group Companies increases, personal data is being transferred between and among them, and across countries and regions, with increasing frequency.

In light of the external and internal environment described above, all Group Companies need to work in the same direction to improve governance of data protection. This will enhance customers' and society's trust in the Group, and lead to expansion of our business and corporate value. With this in mind, NTT DATA Group has established this NTT DATA Group Data Protection Policy ("Policy") which clarifies our position on data protection at the Group level.

2. Purpose and Scope of This Policy

2.1 Purpose of This Policy

Each company of the Group gathers and uses a wide range of information in the course of their normal business operations. This information may include personal data that is protected by data protection laws and regulations.

The purpose of this Policy is to describe the basic principles that govern the processing of personal data at the Group level and the common baseline activities that the Group is required to implement for each Group Company to process personal data appropriately.

We expect this Policy to contribute to the development of a Data Protection Framework (as defined below) for the person or organization responsible for implementing data protection measures at each Group Company.

2.2 Scope of Applicability

This Policy applies to NTT DATA Group and to all Group Companies that process personal data.

2.3 Defined Terms

All capitalized terms not otherwise defined in this Policy have the meanings set forth in Appendix 1.

2.4 Policy Updates

This Policy is subject to ongoing improvement and will be updated as necessary, including changes in the internal and external environment surrounding the Group.

3. Basic Principles

NTT DATA Group has defined the following eight basic principles for data protection ("Basic Principles") that guide the Group on how to protect individual privacy and personal data in the context of increasing international data flows and balancing data protection with the free flow of information across borders in the Group.

- Collection Limitation (Section 3.1)
- Data Quality (Section 3.2)
- Purpose Specification (Section 3.3)
- Use Limitation (Section 3.4)
- Security Safeguards (Section 3.5)
- Openness (Section 3.6)
- Individual Participation (Section 3.7)
- Accountability (Section 3.8)

These Basic Principles have been created in accordance with the principles set forth by the Organization for Economic Cooperation and Development (OECD) in the *Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (2013)*.

3.1 Collection Limitation

Personal data should be collected in a fair and lawful manner, and collected only where necessary for and proportionate to the legitimate business purpose being pursued.

In addition, special care should be taken when collecting personal data of a nature that is considered particularly sensitive, because of the nature of this data, the manner in which it is processed, the context in which it is used, and other circumstances can lead to a violation of rights.

Examples of this principle

- The use of hidden data recording devices, such as tape recorders, or deceiving data subjects to induce them to supply information (e.g., dark patterns) typically is forbidden under many countries' laws and regulations.
- The GDPR states that personal data must be processed lawfully, fairly, and in a transparent manner in relation to the data subject, and collected for specified, explicit and legitimate purposes.
- In principle, the GDPR prohibits the processing of personal data that falls within special categories (e.g., racial or ethnic origin, political opinions, religious or philosophical beliefs), except where more stringent processing requirements are met.
- The CCPA requires that the collection of a consumer's personal information be reasonably necessary and proportionate to achievement of the specified purposes.

- The APPI requires that personal information not be acquired via deception or by other wrongful means, and that when acquiring personal information, the purpose of use of the personal information shall be notified to relevant data subjects or be announced publicly.
- In principle, the APPI prohibits the collection of personal data that is considered sensitive without obtaining consent from the relevant data subject.

3.2 Data Quality

Personal data should be relevant to the purposes for which they are to be used. Also, the accuracy and completeness of personal data collected must be ensured, and the data must be kept up to date, to the extent necessary to achieve the purpose of use of personal data.

In addition, taking into consideration the purposes for which personal data is processed, companies processing personal data should ensure that inaccurate personal data is erased or corrected without delay.

Examples of this principle

- The GDPR requires that the accuracy of personal data be ensured, taking into account the purposes for which the personal data is processed, and mandates that the purposes for which personal data is collected must be specified and legitimate.
- The GDPR also states that personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for purposes of the processing .
- The CCPA requires that the collection, use, retention and sharing of a consumer's personal information be reasonably necessary and proportionate to achievement of the specified purposes.
- Under the APPI, personal information must be processed only within the scope necessary to achieve the specified purposes.
- The APPI requires that efforts be made to keep personal data accurate, taking into account the purposes for which the personal data is processed, and mandates that personal data be processed within the scope necessary for achievement of the specified purposes.

3.3 Purpose Specification

When personal data is processed, the purpose of processing personal data should be clearly specified, taking into account local laws and regulations and the business practices in the relevant country or region, and the personal data should be used within the scope of that purpose.

Personal data may be used for a new purpose only if that purpose is compatible with the original purpose, the consent of the data subject is obtained, or there is a clear basis for the processing pursuant to applicable laws and regulations.

Identification of the purpose of use of personal data will help data subjects who provide their personal data feel comfortable sharing that information with the Group.

Examples of this principle

- The GDPR requires that the purpose of processing be specified, explicit and legitimate.
- The CCPA requires that notice of the purpose for which relevant categories of personal information are collected shall be provided at or before the point of collection.
- The APPI requires that the purpose of use of personal information be specified as much as possible.

3.4 Use Limitation

Personal data should not be processed for purposes other than those specified, in accordance with Section 3.3, except: a) with the consent of the data subject, or b) as permitted by applicable laws and regulations.

Any use of personal data beyond the scope of identified purposes is a violation of laws and regulations in each country and region. Violations will cause customers and society to lose trust in the Group.

With certain exceptions (for example, when a data subject has given consent or when permitted by applicable laws and regulations), personal data must be used within the scope of the purposes of use specified in accordance with Section 3.3.

Examples of this principle

- Under the GDPR, personal data must be collected for specified purposes and not further processed in a manner that is incompatible with those purposes.
- Under the CCPA, using collected personal information for additional purposes that are incompatible with the disclosed purpose(s) for which the personal information was collected is not permitted unless the relevant data subject is provided with notice thereof, in form and content consistent with the CCPA.
- Under the APPI, personal information must be processed only within the scope necessary to achieve the specified purposes, and may not be provided to a third party without obtaining prior data subject consent.

3.5 Security Safeguards

Personal data should be protected by reasonable security safeguards, such as administrative, technical and physical controls, to protect against risks like loss, destruction, or unauthorized access to or use, modification, or disclosure of personal data.

There is a common expectation that all businesses that process personal data will ensure the security of that personal data. The Group provides services using information technology, so we need to take security measures to protect personal data in a careful manner.

When considering security measures, it is expected that the laws, regulations, and business practices in each relevant country and region will be taken into account.

Examples of this principle

- Technical measures generally include encryption, pseudonymization and anonymization.
- Organizational measures typically include creating an internal security policy, which requires employees to limit the amount of personal data collected or to delete personal data that no longer is needed.
- The GDPR mandates that personal data must be processed in a manner that ensures appropriate security of the relevant data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures and also states that, if applicable, appropriate data processing agreements shall be executed with data processors.
- The CCPA requires the implementation of reasonable security procedures and practices appropriate to the nature of the personal information, to protect the personal information against unauthorized or illegal access, destruction, use, modification, or disclosure, and also requires, if

applicable, the execution of an appropriate data processing agreement with a service provider or contractor.

- Under the APPI, necessary and proper measures for the prevention of leakage, or loss of, or damage to personal data, as well as other security controls on personal data, must be implemented, and it is necessary to supervise employees and contractors.

3.6 Openness

When processing personal data, there should be a general policy of transparency about practices and policies relating to personal data.

Enhancing the transparency of information that relates to the processing of personal data, including policies on the processing of personal data and the purposes for which personal data is used, will not only reassure the data subjects who share their personal data with us, but also contribute to society trusting that the Group manages personal data appropriately.

Based on the above, data subjects must be notified of necessary information such as the processing of personal data, the purpose of its use, and information on Controllers, in accordance with applicable laws and regulations. When processing personal data on behalf of a Data Controller, each Group Company should act on the instructions of the Data Controller in response to requests from data subjects.

Even where specific measures related to this principle are not required by laws and regulations, increased transparency of information relating to the processing of personal data is encouraged.

Examples of this principle

- A privacy notice describing the processing of personal data is provided to data subjects in a clear and accessible manner at the time that their personal data is collected or shared.
- The GDPR requires that personal data be processed in a transparent manner in relation to the data subject.
- The CCPA requires that a Data Controller which collects personal information is required to provide relevant information prominently and conspicuously on the homepage of its internet website in accordance with the CCPA and its sub-regulations.
- The APPI requires that the following items be made accessible to data subjects (including situations in which a response is made, without delay, at the request of a data subject):
  (1) the name of the business operator processing personal information;
  (2) the purpose of use of all retained personal data;
  (3) procedures to comply with data subjects' requests to exercise their rights; and (4) measures to manage the security of all retained personal data and other relevant information.
- The PIPL requires that the following items must be included in a privacy notice (please note that other items also need to be included to comply with the PIPL):
  (1) the name and contact information of the Data Controller;
  (2) the purposes and methods of processing;
  (3) the categories of personal information to be processed;
  (4) the period for which the personal information is retained; and
  (5) for data transfers outside of China, the name and contact information of the data recipients, the purposes and methods of processing by those recipients, the types of personal information to be transferred, and the method and procedure by which data subjects can exercise their rights under the PIPL with respect to the personal information transferred to recipients.

3.7 Individual Participation

Data protection laws and regulations generally give data subjects several rights, for example, the right in relation to their personal data to be able to verify the location and content of their personal data concerning them and the right to object to the Data Controller's processing of their personal data.

Therefore, in accordance with applicable laws and regulations, the Group should ensure that data subjects are in a position to exercise their rights. In addition, we expect that the Group will act to enforce and uphold data subjects' rights in accordance with applicable laws and regulations, without undue delay.

Examples of this principle

- The GDPR provides individuals with rights to access, rectify, and erase personal data, and to restrict processing, data portability, to object to processing, and not to be subject to a decision based solely on automated processing.
- The CCPA provides California residents with the following major privacy rights:
  (1)Right to delete;
  (2)Right to correct;
  (3)Right to know;
  (4)Right to opt-out of sale or sharing;
  (5)Right to limit use and disclosure of sensitive personal information; and (6) Right to non-discrimination.
- The APPI provides individuals with rights to disclose, correct, add, delete, discontinue use of, erase, and discontinue provision of all retained personal data.

3.8 Accountability

The Basic Principles above need to be complied with when processing personal data as a Data Controller.

Under this principle, responsibility for compliance with applicable data protection laws and regulations should be placed on the Data Controller, who is not relieved of this obligation simply because the processing of personal data is carried out by a third party on its behalf.

In addition, there is an expectation of compliance with the Basic Principles above even when processing personal data on behalf of a Data Controller, in which case compliance should be managed in close cooperation with the Data Controller.

Examples of this principle

- Under the GDPR, the APPI and the CCPA, entrusting a third party with the processing of personal data does not exempt a Data Controller from liability for compliance with the law, and if the third party violates the law, the Data Controller will be held liable.
- The GDPR requires Data Controllers to comply with the basic principles set forth therein and to be able to demonstrate compliance with them.

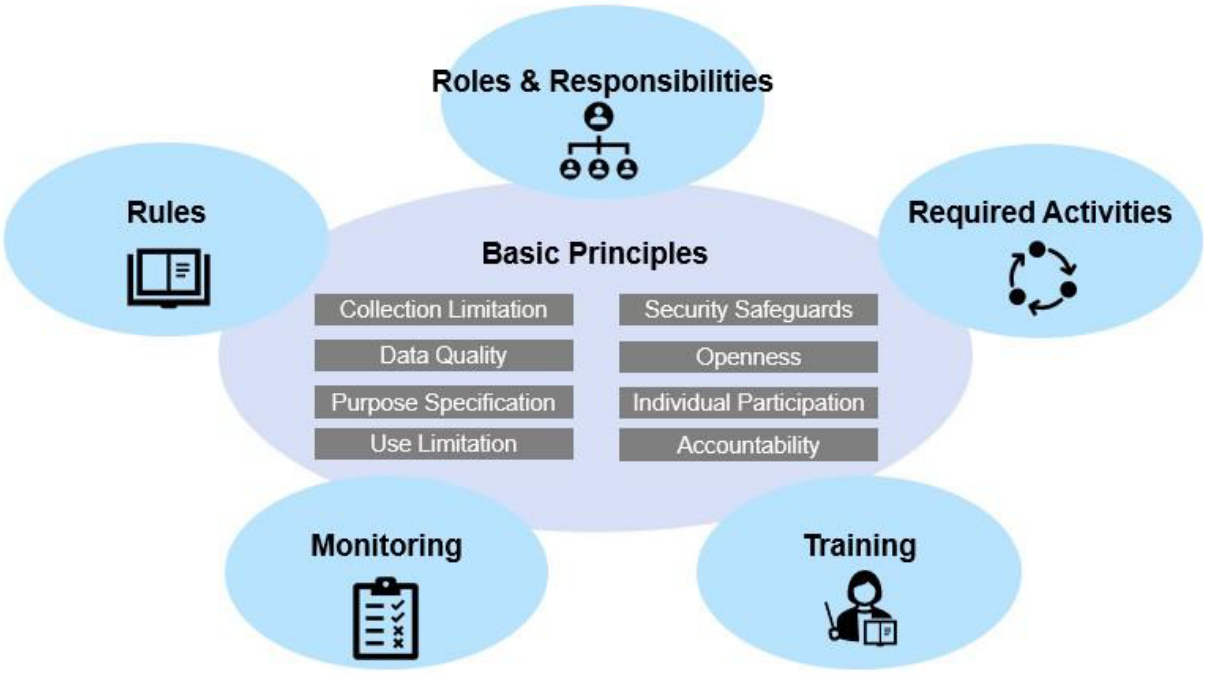
4. Data Protection Framework

In order to avoid or reduce the serious impact caused by noncompliance with data protection laws and regulations, the Group has established the framework described below ("Data Protection Framework") to manage data protection properly, based on the Basic Principles, and subject to compliance with applicable laws and regulations in each relevant country and region.

Figure 1 outlines the Data Protection Framework, which is comprised of the following main components and is designed to reduce negative impact on the management and operations of the Group and to enable the management of the Group to make appropriate decisions with regard to data protection.

- Rules (Section 5)
- Roles and Responsibilities (Section 6)
- Required Activities (Section 7)
- Training (Section 8)
- Monitoring (Section 9)

Figure 1: Data Protection Framework



5. Rules

It is essential to promote data protection by establishing policies and rules that define what the Group's employees must do when processing personal data.

NTT DATA Group has created this Policy to clarify the Basic Principles of data protection at the Group level, and the baseline obligations to be implemented by all Group Companies. A checklist is provided in Appendix 2, as a reference for each Group Company, to confirm compliance with this Policy.

NTT DATA Japan, NTT DATA, Inc., and each Unit Headquarter must establish internal data protection rules that set forth the matters and processes with which its employees must comply when processing

personal data. No Group Company may establish data protection rules and procedures that deviate from this Policy, except where stricter data protection rules and procedures are established.

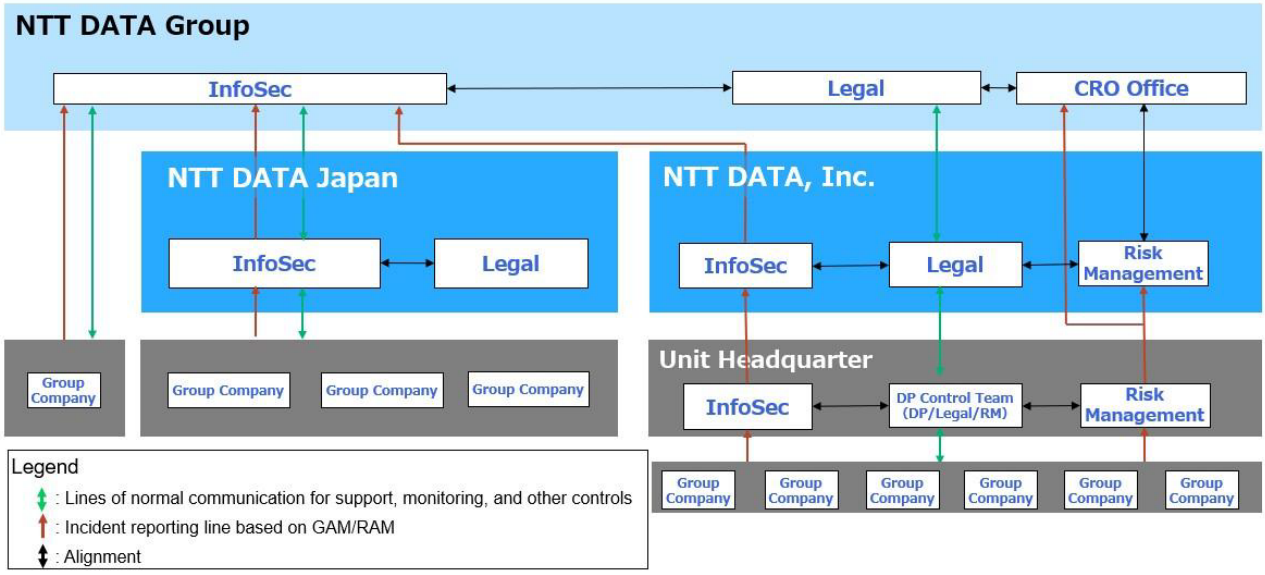
NTT DATA Japan, NTT DATA, Inc. and each Unit Headquarter must submit the latest versions of their internal data protection rules and procedures to NTT DATA Group (or to NTT DATA, Inc. in case of each Unit Headquarter), at least on an annual basis.

6. Roles and Responsibilities

To ensure adequate data protection, in addition to clarifying the person responsible for ensuring that personal data is processed in accordance with this Policy in each organization that processes personal data, NTT DATA Japan, NTT DATA, Inc., and each Unit Headquarter is required to procure the responsible person(s) and functions internally, and to secure the necessary resources to promote data protection.

Figure 2 demonstrates the organizational structure of the Group for purposes of promoting data protection.

Figure 2 Group-wide Data Protection Organizational Structure



The roles and responsibilities of NTT DATA Group, NTT DATA Japan, NTT DATA, Inc., and each Unit Headquarter are described below.

Company	Roles and Responsibilities

NTT DATA Group	• Developing and maintaining this Policy as the owner • Developing and implementing internal data protection rules for NTT DATA Group • Developing and operating escalating rules for serious personal data incidents at the Group level in accordance with Section 7.7. • Implementing the processes described in Section 7 • Training its employees on data protection • Monitoring the Group in accordance with Section 9 and assessing data protection risks for the Group • Leading cross-group data protection initiatives and resolving common Group issues related to data protection • Providing support to NTT DATA Japan and NTT DATA, Inc. with regard to data protection
NTT DATA Japan	• Appointing a person to be responsible for data protection at NTT DATA Japan • Developing and implementing internal data protection rules for NTT DATA Japan and its subsidiary companies • Implementing the processes described in Section 7 and getting its subsidiary companies to implement those processes as well • Training its employees, and getting its subsidiary companies to train their employees, on data protection • Monitoring its organization and its subsidiary companies in accordance with Section 9 • Providing support to its subsidiary companies with regard to data protection
NTT DATA, Inc.	• Appointing a person to be responsible for data protection at NTT DATA, Inc. • Developing and operating internal data protection rules for NTT DATA, Inc. • Implementing the processes described in Section 7 • Training its employees on data protection • Monitoring its organization and each Unit Headquarter in accordance with Section 9 • Supporting each Unit Headquarter with regard to data protection
Unit Headquarters	• Appointing a person responsible for data protection at each Unit Headquarter • Developing and operating internal data protection rules for each Unit Headquarter and its subsidiary companies • Implementing the processes described in Section 7 and getting its subsidiary companies to implement such processes • Training its employees on data protection and getting its subsidiary companies to train their employees • Monitoring its organization and its subsidiary companies in accordance with Section 9

	・ Supporting its subsidiary companies with regard to data protection
Group Companies other than the above companies	・ Performing control activities related to data protection in accordance with the instructions of the company (NTT DATA Group, NTT DATA Japan, NTT DATA, Inc., or each Unit Headquarter) that directly manages its Group Company

7. Required Activities

Based on the Basic Principles, this Section describes the baseline for what each Group Company must implement when processing personal data.

7.1 Legitimate Notice

When collecting and processing personal data, the Transparency and Accountability Basic Principles require that each Group Company make disclosures concerning the contents and purpose of the personal data processed to data subjects at the time that their personal data is collected and shared, or as soon as possible thereafter.

If each Group Company is a Data Controller, it must notify data subjects of information related to the processing of their personal data for which disclosure is required by applicable laws and regulations.

NTT DATA Group and each Group Company must ensure that all of the aforementioned notices and disclosures are prepared and provided in a manner that is clear, accurate, complete, and accessible, so that individuals can understand their contents.

7.2 Record of Collection and Processing

In order to comply with laws and regulations and to fulfill the Accountability Principle, it is important to maintain a situation in which each Group Company can track the collection and processing of personal data within the company.

Therefore, each Group Company must keep records of the information related to the processing of personal data, at least to the extent required by applicable laws and regulations.

The following examples of the items that should be recorded by organizations processing personal data are provided as a reference for the development of company rules for recording information at each Group Company: ・ Project name / Corporate division;

- The person(s) responsible for the project and the contact person(s);
- Purpose of use and/or processing of personal data;
- Categories and content of personal data;
- The country/region to which the personal data will be transferred; and ・ The period for which personal data will be retained.

7.3 Security Measures

Data subjects and society expect that companies processing personal data ensure the confidentiality, integrity and availability of personal data.

When processing personal data, each Group Company must implement technical and organizational security measures, in accordance with applicable laws and regulations, as well as applicable group policies and rules such as NTT DATA Group Security Policy (GSP). In addition, when processing personal data of a third party, such as a customer, NTT DATA Group and each Group Company must confirm whether the security obligations in the relevant contract can be satisfied before executing the contract.

Examples of typical security measures are set forth in Appendix 3, for consideration by each Group Company.

7.4 Third Party Management

Many Group Companies work with third parties such as suppliers and subcontractors that process personal data on their behalf or to whom personal data is transferred. Appropriate management of third parties with regard to data protection reduces risks, such as a leak or misuse of personal data.

To ensure proper third-party risk management, each Group Company must satisfy the following prerequisites when personal data is transferred to a third party and/or have a third party process such personal data on its behalf,:

- Confirm whether the third party meets the security requirements established by the Data Controller and/or the relevant Group Company, and/or the requirements in applicable laws and regulations;
- Execute a contract governing the processing of personal data, if required by applicable laws and regulations; and
- Periodically monitor whether the third party continues to satisfy and comply with the security requirements.

7.5 Requests from Data Subjects

Data protection laws and regulations in many countries and regions require each Group Company to ensure that data subjects can exercise their rights, as set forth in Section 3.7.

If a data subject makes a complaint, requests a consultation, or makes another request relating to the processing of personal data, each Group Company must respond in an appropriate manner, without undue delay.

In order to ensure an appropriate response, NTT DATA Japan, NTT DATA, Inc. and each Unit Headquarter must organize and document its processes for responding to data subjects in accordance with applicable laws and regulations.

7.6 Response to Breaches

It is essential to manage Incidents properly, to prevent damage to the Group's corporate value. “Incident” means a leak of personal data, the use of personal data for unauthorized purposes, or other forms of noncompliance with applicable laws and regulations in each relevant country and region.

If an Incident occurs, each Group Company must promptly take measures to prevent further damage to prevent negative effects of the Incident from worsening and must respond promptly and appropriately to the affected data subjects and regulatory authorities in accordance with applicable laws and regulations and relevant contracts with customers. To respond to Incidents appropriately, NTT DATA Japan, NTT DATA, Inc., and each Unit Headquarter must organize and document their respective processes for responding to Incidents, based on applicable laws and regulations.

In addition, NTT DATA Japan, NTT DATA, Inc. and each Unit Headquarter must report an Incident to NTT DATA Group (or to NTT DATA, Inc. in case of each Unit Headquarter) immediately, if the Incident occurs at itself or its subsidiary companies and requires escalation to NTT DATA Group in accordance with the escalation rules set forth in the Group Authority Matrix, including the Security Incident Response Standard.

7.7 Cross-Border Transfers

Although some data protection laws and regulations, such as the GDPR, the PIPL and the APPI, restrict the transfer of personal data across borders, to different countries and regions, it is extremely important for the Group to comply with these cross-border transfer regulations properly.

When transferring personal data outside of the country in which it originates, each Group Company must comply with applicable laws, regulations and contractual requirements (e.g., entering into a standardized contract for the transfer and implementing appropriate technical measures).

8. Training

Employees who process personal data need to be aware of the importance of data protection, and we must foster a culture of respect for data protection within the Group.

Therefore, each Group Company must provide training and/or educational opportunities on data protection to its employees at least once a year, based on applicable laws and regulations.

9. Monitoring

NTT DATA Group, NTT DATA Japan, NTT DATA, Inc., and each Unit Headquarter must implement the following monitoring of their respective organizations and their subsidiary companies.

■Monitoring of each company

NTT DATA Group	NTT DATA Group must confirm the following matters of its organizations and Group Companies via NTT DATA Japan and NTT DATA, Inc., at least on an annual basis: - Status of establishment of NTT DATA Japan's, NTT DATA, Inc.'s and each Unit Headquarter's internal data protection rules and procedures - Status of employee training on data protection - Status of compliance with applicable laws and regulations Where any Group Company with a high data protection risk is identified, NTT DATA Group will check the control status of that Group Company and seek improvement if necessary.

NTT DATA Japan	NTT DATA Japan must confirm the following matters of its organizations and its subsidiary companies, at least on an annual basis: - Status of establishment of internal data protection rules and procedures of its subsidiary companies - Status of employee training on data protection - Status of compliance with applicable laws and regulations NTT DATA Japan must submit the latest version of its data protection rules and procedures (“個人情報保護規程” and “日本地域個人情報保護規程”) to NTT DATA Group in accordance with Section 5.
NTT DATA, Inc.	NTT DATA, Inc. must cooperate with the monitoring and assessment regularly conducted by NTT DATA Group and confirm the following matters of its organizations and its subsidiary companies, at least on an annual basis: - Status of establishment of each Unit Headquarter’s internal data protection rules and procedures - Status of employee training on data protection - Status of compliance with applicable laws and regulations NTT DATA, Inc. must submit the latest version of the data protection rules and procedures of NTT DATA, Inc. and all Unit Headquarters to NTT DATA Group in accordance with Section 5.
Unit Headquarters	Each Unit Headquarter must cooperate with the monitoring and assessment regularly conducted by NTT DATA Group and NTT DATA, Inc. and confirm the following matters of its organizations and its subsidiaries, at least on an annual basis: - Status of employee training on data protection - Status of compliance with applicable laws and regulations Each Unit Headquarter must submit the latest version of its data protection rules and procedures to NTT DATA, Inc. in accordance with Section 5.

10. Group Alignment

In order to promote data protection at the Group level, it is expected that NTT DATA Group, NTT DATA Japan, NTT DATA, Inc. and each Unit Headquarter will collaborate with one another actively, for example, by exchanging information relating to the latest amendments to data protection laws and regulations.

To ensure the smooth, lawful transfer of personal data among the Group, NTT DATA Group encourages all Group Companies transferring personal data across national boundaries to and from other Group Companies to participate in the framework of the NTT DATA Group Transfer Agreement (“IGTA”), which is a comprehensive agreement among the Group relating to transfers of personal data. Supplementary Provisions

As of April 1, 2024: Unit Headquarters must comply with the obligations set forth in Sections 5 , 6, 7, 8, and 9 of this Policy effective April 1, 2025.

Appendix 1 Definitions

No	Terms	Definitions
1	Data Controller	A party that, alone or jointly with others, determines the purposes and means of processing of personal data and similar terms under applicable laws and regulations.
2	Group	NTT DATA Group and its subsidiary companies
3	Group Company	A subsidiary company of NTT DATA Group
4	Incident	A leak of personal data, use of personal data for unauthorized purposes, or other violation of applicable laws and regulations in each relevant country and/or region.
5	NTT	Nippon Telegraph and Telephone Corporation, a company located in Japan.
6	NTT DATA Japan	NTT DATA Japan Corporation, a company located in Japan, owned by NTT DATA Group.
7	NTT DATA Group	NTT DATA Group Corporation, a company located in Japan.
8	NTT DATA, Inc.	NTT DATA, Inc., a company located in Japan, owned by NTT DATA Group and NTT.
9	Unit Headquarter	An operating company that manages a region or solution, which is defined by NTT DATA, Inc. for group management purposes.
10	Policy	NTT DATA Group Data Protection Policy

Appendix 2 Common Checklist

No	Category	Questions	Y/N
1	Rules	Does your company have any company rules specifically for data protection?	
2	Roles and Responsibility	Is there any person who has overall responsibility for data protection at the company or your group level?	
3	Required Activities	As a Data Controller, has your company prepared a privacy notice or statement for all relevant data subjects such as customers and employees when processing personal data?	
4		Does your company require employees to keep and update records of information required by applicable data protection laws and regulations?	
5		Does your company take security measures to protect personal data in accordance with laws and regulations, and the internal security policy and rules?	
6		When personal data is transferred to a third party and/or a third party processes personal data on your behalf, does your company confirm whether the third party's security management system meets the relevant security requirements, as defined by the Data Controller or your company?	
7		When personal data is transferred to a third party and/or a third party processes personal data on your behalf, does your company execute a contract regarding the processing of personal data?	
8		When personal data is transferred to a third party and/or a third party processes personal data on your behalf, does your company regularly monitor the third party?	
9		Does your company organize and document its processes for responding to a complaint, consultation, or request from data subjects regarding the processing of personal data?	
10		Does your company organize and document its processes to respond to Incidents?	
11		When personal data is transferred outside the country of origin, does your company ensure there is a lawful basis for doing so?	

12	Training	Does your company provide training and/or educational opportunities on data protection to all your employees at least once a year?	
13	Monitoring	Does your company periodically monitor compliance with data protection laws and regulations by your organizations that process personal data?	

Appendix 3 Sample Security Measures

- Measures for pseudonymization and encryption of personal data
- Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services
- Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
- Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of processing
- Measures for user identification and authorization
- Measures for the protection of data during transmission
- Measures for the protection of data during storage
- Measures for ensuring physical security of locations at which personal data is processed
- Measures for ensuring event logging
- Measures for ensuring system configuration, including default configuration
- Measures for internal IT and IT security governance and management
- Measures for certification/assurance of processes and products
- Measures for ensuring data minimization
- Measures for ensuring data quality
- Measures for ensuring limited data retention
- Measures for allowing data portability and ensuring erasure

NTT DATA Group Data Protection Policy

April 1st, 2024

Revised July 1st, 2025

NTT DATA Group Corporation