Technical and Organizational Measures

At NTT it is our vision, **through technology and innovation**, to enable a **secure and connected future**. We have established our NTT Technical and Organizational Measures ('TOMs') that describe how we ensure the protection of personal data in a transparent, fair, ethical and lawful way.

Our TOMs are based on industry best practices and applicable legal requirements in jurisdictions in which we operate taking into account the nature of the data we process and cost of implementation.

Contents

A.	**Data Privacy and Protection Measures**	**04**
1	Governance and Operating Model	04
2	Policies, processes and Guidelines	04
3	Data Protection by Design	04
4	Data Landscape	04
5	Information Lifecycle Management	04
6	Data Privacy and Protection Training and Awareness	05
7	Security for Privacy	05
8	Breach Response and Notification	05
9	Third Party Management	05
10	Monitor and Assess	05
B.	**Information Security Measures**	**05**
11	Information Security	05
12	Human Resources	06
13	Access Controls	06
14	Asset Management	06
15	Physical and Environmental Security	06
16	Operational Security	07
17	System Acquisition, Development and Maintenance	07
18	Third Party Management	07
19	Information Security Incident Management	07
20	Business Continuity	08
21	Compliance	08

(A) Data Privacy and Protection Measures

1 Governance and Operating Model

1.1 NTT is committed to demonstrating accountability when NTT processes personal data and have implemented an organizational structure, and roles and responsibilities for managing and providing oversight over the processing of personal data.

1.2 A number of governance structures have been implemented to ensure that data privacy and protection matters are reviewed by appropriate management within NTT. Ultimate accountability for data privacy and protection is held by the NTT Ltd Board and is supported by designated roles throughout the business, including appointed Data Protection Officers or equivalent roles, where required under Data Protection Laws.

2 Policies, processes and Guidelines

2.1 NTT has implemented and communicated its policies, processes, standards and guidelines that detail how NTT employees are expected to process personal data. This includes the following policies:

2.1.1 Data Privacy and Protection Policy;

2.1.2 Data Subject Rights Policy; and

2.1.3 Personal Data Breach Notification Policy.

2.2 NTT has defined and communicated privacy notices that provide information to employees, clients and other stakeholders about how personal data is processed.

2.3 NTT has a Data Protection Impact Assessment ('DPIA') Process and performs DPIAs when required and in accordance with Data Protection Laws.

3 Data Protection by Design

3.1 NTT is committed to implementing reasonable measures to support its clients' ability to comply with Data Protection Laws. As far as possible, the principles of data protection by design and by default are applied during the development and delivery of NTT products, services and solutions.

4 Data Landscape

4.1 NTT has implemented processes to identify, record, assess and maintain an understanding of the personal data that NTT processes.

4.2 NTT maintains a record of the personal data processed in accordance with applicable Data Protection Laws.

5 Information Lifecycle Management

5.1 NTT has implemented policies and processes to ensure that personal data is processed appropriately throughout its lifecycle (from collection through to use, retention, disclosure and destruction).

5.2 Data Protection Laws, in certain countries, provide data subjects with specific rights in relation to their personal data. NTT is committed to upholding these rights and ensuring that NTT responds to data subject requests in a transparent, fair, ethical and lawful way.

5.3 NTT has implemented a Data Subject Rights Policy and Data Subject Requests Process to uphold data subject rights in accordance with applicable Data Protection Laws.

5.4 NTT maintains a record of all data subject requests received and the actions taken to respond to these requests. NTT will provide all reasonable support to clients in responding to data subject requests, where requested, and in accordance with the agreements with them.

5.5 NTT maintains a Data Retention Policy and Schedule which is aligned to applicable laws. NTT only retains personal data where there is a legitimate business purpose and in accordance with its obligations under law. NTT destroys, deletes or de-identifies personal data when the retention period lapses and there is no legitimate business reason to retain the personal data for a longer period.

5.6 NTT keeps the personal data processed on behalf of its clients in accordance with client requirements and will destroy, delete, de-identify or return personal data when requested, to the client, and where there are no further obligations to retain the personal data under applicable law.

5.7 NTT has implemented all reasonable efforts to ensure that personal data is accurate, complete and up to date.

5.8 NTT relies on Standard Contractual Clauses to support the lawful transfer personal data outside of the country where it was originally collected and have appropriate agreements in place with NTT subsidiaries, affiliates, processors, sub-processors and clients to support cross-border transfers.

6 Data Privacy and Protection Training and Awareness

6.1 NTT requires all employees to complete data privacy and protection training on an annual basis. All data privacy and protection policies, processes, standards and guidelines are available to employees and communicated regularly. Where required, local, regional or functional training is also provided to support employees to act in line with data protection requirements in specific countries, regions or business functions.

7 Security for Privacy

7.1 NTT data privacy and protection and information security teams work together to ensure that appropriate data protection governance and control is implemented to protect the confidentiality, integrity and availability of personal data.

Our security methodologies are aligned to ISO27001 and NIST Cyber Security Framework ('CSF').

8 Breach Response and Notification

8.1 NTT has policies, processes and procedures for identifying, detecting, responding, recovering and notifying appropriate stakeholders in the event of a personal data breach. This includes mechanisms for performing a root cause analysis and undertaking corrective actions.

8.2 NTT is committed to ensuring that NTT notifies applicable data protection authorities, affected clients and affected data subjects in the event of a personal data breach in compliance with applicable Data Protection Laws and any contractual commitments.

8.3 NTT maintains a record of all personal data breaches and the actions taken to respond to these events.

8.4 NTT incident management measures to identify, detect, respond and recover from information security incidents are outlined in Section B (Information Security) of these TOMs.

9 Third Party Management

9.1 NTT is accountable for the actions of its processors (i.e. sub-processors) who process personal data on NTT's behalf and assesses the ability of our processors to protect personal data at the time of selection and on a periodic basis thereafter in accordance with NTT policies.

9.2 NTT processors are required to sign appropriate agreements that govern the processing and protection of personal data and require the same obligations, as outlined in the Data Processing Agreement, to be transferred to any further processors who NTT may engage. NTT has undertaken all reasonable efforts to ensure that Data Processing Agreements are in place with its processors.

10 Monitor and Assess

10.1 NTT reports on the design and operational effectiveness of its data privacy and protection activities to the NTT Ltd Audit and Risk Committee and senior management on a periodic basis. This includes dashboard reporting, management self–assessments, certifications, internal audit reviews and independent audits and assessments.

(B) Information Security Measures

NTT is committed to ensuring that information security control is implemented and properly managed, in order to protect the confidentiality, integrity and availability of personal data processed on behalf of and under the instruction of of its clients.

NTT has established a group wide Information Security Management System ('ISMS') which is aligned to leading information security practices and standards from around the world including the ISO27000 series and NIST Cyber Security Framework ('CSF').

11 Information Security

11.1 Roles and responsibilities for information security have been formally assigned, with reporting lines which ensure the independence of the function, including a Chief Security Officer ('CSO'), Chief Information Security Officers ('CISO'), and Information Security Officers ('ISO').

11.2 NTT employees are responsible for ensuring that they act in accordance with the information security policies, processes, standards and guidelines in their day-to-day business activities.

11.3 NTT has documented and published a set of information security policies that support the requirements of the ISMS. Policies and supporting documentation are reviewed periodically.

11.4 NTT has measures in place to ensure that mobile devices (including laptops, mobile phones, tablets, devices allowing remote access and 'Bring Your Own Device' schemes) and their contents are protected. Reasonable efforts have been undertaken by NTT to ensure that mobile device management ('MDM') software is installed on all mobile devices with access to the NTT corporate network.

11.5 Teleworkers are only able to remotely access the NTT infrastructure through the use of Virtual Private Network ('VPN') services, where possible.

12 Human Resources

12.1 NTT performs background and employment screening for its employees, to the extent permitted under applicable law, to ensure their suitability for hiring and handling company and client information (including personal data). The extent of the screening is proportional to the business requirements and classification of information that the employee will have access to.

12.2 NTT requires that NTT employees (including contractors and temporary employees) agree to maintain the confidentiality of NTT's internal and client data (including personal data).

12.3 NTT employees are required to complete information security awareness training on an annual basis. Information security policies and supporting procedures, processes and guidelines are made available to employees and employees receive relevant information about trends, threats and best practices through NTT communication platforms.

13 Access Controls

13.1 NTT has an Acceptable Use Policy that supports the proper and effective use and protection of NTT corporate assets, including computer and telecommunication resources, products, services, solutions and IT infrastructure.

13.2 NTT has an Information Classification Policy that describes the appropriate technical and organizational controls for handling information based on its classification. Information and assets are protected in line with the classification label.

14 Asset Management

14.1 NTT has an Access Control Policy, supporting procedures and logical and physical access measures, to ensure that only authorized persons have access to information based on the principle of least privilege.

14.2 Access reviews are periodically performed on IT assets, applications, systems and databases to ensure only authorized individuals have access.

14.3 NTT processors (i.e. sub-processors) must access NTT systems using named accounts. Generic accounts and/or sharing of credentials is prohibited unless an exception is expressly authorized by management or clients.

14.4 NTT has undertaken reasonable efforts to strictly limit the number of privileged ('Admin') users on its applications, systems and databases.

15 Physical and Environmental Security

15.1 NTT has implemented reasonable and appropriate measures in line with the Physical Security Policy to prevent unauthorized physical access, damage or interference with NTT information, applications, systems, databases and infrastructure across the following domains:

15.1.1 Physical access controls;

15.1.2 Monitoring and auditing of physical access;

15.1.3 Protection from environmental hazards;

15.1.4 Securing physical assets;

15.1.5 Cabling security;

15.1.6 Handling physical and informational assets;

15.1.7 Maintenance and disposal of physical assets;

15.1.8 Clear desk and screen practices;

15.1.9 Visitors access and supervision; and

15.1.10 Health and safety procedures.

16 Operational Security

16.1 The NTT Information and Technology ('I&T') function is responsible for managing NTT applications, systems, databases and infrastructure. I&T documents, maintains and implements all IT operational policies and procedures that are aligned to COBIT and ITIL standards.

16.2 NTT has a policy and supporting procedures for managing changes to our business processes, applications, systems, databases and infrastructure. NTT has established several governance structures to review and approve any changes based on the size and scope of the change and strategic objectives. All requests and their outcomes are logged and documented.

16.3 NTT has established a threat and vulnerability management programme supported by industry standard tools for identifying, managing and mitigating risks to company information including the personal data of employees and clients. This includes next generation Endpoint Detection and Response ('EDR') for Anti-Virus and Anti-Malware tools, regular scanning of environments, patching protocols and management of remediation and improvement activities.

16.4 Capacity requirements are continuously monitored and regularly reviewed. Systems and networks will be managed and scaled in line with these reviews.

16.5 System availability includes architecture, high-availability design, and/or backups based on the risk and availability requirements for each system. The method for maintaining system availability or recovery, including the scope and frequency of back-ups is determined based on NTT business requirements, including client requirements, and the criticality of the information. Monitoring of backups is performed to ensure the successful completion of back-ups, as well as manage any back up issues, exceptions or failures.

16.6 NTT apply reasonable efforts to maintain audit logging on applications and systems. Logs are periodically reviewed and are available for investigation purposes. Access to logs is strictly limited to authorized personnel only.

17 System Acquisition, Development and Maintenance

17.1 NTT has a Security Architecture and Design Policy and supporting standards and procedures to ensure that security by design principles are applied within the software development life-cycle.

17.2 NTT does not allow production, client, personal data or any confidential information to be used for testing purposes. In exceptional cases, production or client data may be used with the approval of the relevant client or business owner.

18 Third Party Management

18.1 NTT has a Third Party Security Policy and supporting procedures to ensure that information assets are protected when NTT engages third party service providers and/or processors. This includes requirements for information security due diligence and information security risk assessments to be performed, in order to ensure:

18.1.1 Information Security requirements are clearly articulated and documented in the agreements with NTT processors;

18.1.2 NTT processors implement the same level of protection and control as NTT;

18.1.3 Processors are required to report any suspected or actual information security incidents to NTT in a timely manner.

18.2 NTT has undertaken reasonable efforts to ensure that appropriate agreements are in place with processors who have access to NTT information, applications, systems, databases and infrastructure. These agreements include NTT information security standards for ensuring the confidentiality, integrity and availability of NTT information.

19 Information Security Incident Management

19.1 NTT has policies, processes and procedures for identifying, detecting, responding, recovering and notifying appropriate stakeholders in the event of an information security incident, including personal data breaches. This includes mechanisms for performing a root cause analysis and undertaking corrective actions.

19.2 NTT has established group wide security operations to proactively monitor and manage all network and computing assets. This is supported by technical tools for information security incident response and recovery.

20	**Business Continuity**	**21**	**Compliance**	21.2	NTT is driving a consistent approach to information security across its business operations. NTT products, services and solutions are aligned to the ISO 27001 standard and, where certified as outlined in the Client Agreement, are audited on an annual basis in accordance with this standard
20.1	NTT has established business continuity and disaster recovery plans. NTT has adopted a layered approach to ensure the availability of our systems and data.	21.1	NTT has established roles and responsibilities for identifying laws and regulations that affect NTT business operations. Responsibility for compliance with laws and regulations are established at a group and regional level to ensure NTT meets global and local requirements.		

For any questions, please reach out to the Privacy Office at **privacyoffice@global.ntt**

Together we do great things