NTT DATA

Technical and organizational measures

NTT Limited

“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 the cost of implementation.

If you have any questions about our TOMs or how they relate to our products, services and solutions, please contact us at privacyoffice@global.ntt

Content

A DATA PRIVACY AND PROTECTION MEASURES

Content

B INFORMATION SECURITY MEASURES

Content

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 has implemented an organizational structure, roles and responsibilities for managing and providing oversight for the processing of personal data.

1.2 Several 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 in our business is held by the NTT Ltd. Board and is supported by designated roles throughout the business, including Data Protection Officers or equivalent roles.

1.3 NTT reports on the design and operating effectiveness of its data privacy and protection activities to the NTT Ltd. Audit and Risk Committee periodically.

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:

a. Data privacy and protection policy
b. Data subject rights policy
c. 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 following applicable 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 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 it 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 NTT maintains a data retention policy and schedule, which is aligned with applicable laws.NTT only retains personal data where there is a legitimate business purpose and in accordance with its obligations under the 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.

5.3 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 and where there are no further obligations to retain the personal data under applicable law.

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

6. Data subject rights

6.1 Data protection laws in certain countries provide data subjects with specific rights about 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.

6.2 NTT has implemented a Data Subject Rights Policy and Data Subject Requests Process to uphold the data subject rights in accordance with applicable data protection laws.

6.3 NTT supports the following data subject rights:
a. right to be informed;
b. right of access;
c. right to rectification;
d. right to be forgotten;
e. right to data portability;
f. right to restrict use;
g. right to object (including the right to opt-out of direct marketing and the sale of personal data);
h. right to challenge automated decisions; and
i. right to complain.

7.4 NTT maintains a record of all data subject requests received and the actions taken to respond to these requests.

6.5 NTT will provide all reasonable support to clients in responding to data subject requests, where requested, and in accordance with our agreements with them.

6.6 NTT is committed to ensuring that we respond to all requests from public authorities to access personal data in accordance with applicable laws, and where permitted uphold and enforce the rights and freedoms of individuals. Where requests are made of NTT to disclose personal data, NTT does so in accordance with its Public Authority Data Request Policy and maintains a record of these requests and publishes these in an annual transparency report.

7. Cross-border transfers

7.1 NTT relies on Standard Contractual Clauses to support the lawful transfer of personal data from the European Union or from the United Kingdom to third countries and has appropriate agreements in place with NTT subsidiaries, affiliates, processors, sub-processors, and clients to support cross-border transfers. Where required, NTT may also request consent from data subjects for the cross-border transfer of their personal data.

7.2 Where personal data is transferred across borders, NTT performs transfer impact assessments to determine whether the country to which personal data is transferred offers the same level of protection to the rights and freedoms of data subjects as the original country. Where gaps are identified, NTT has implemented supplementary measures to support data subject rights in accordance with its policies and ensure that personal data is processed in a transparent, fair and ethical way.

8. Regulatory

8.1 NTT is committed to keeping abreast of changes to data protection laws in the countries in which NTT operates and has implemented processes to support compliance.

9. Training and awareness

9.1 NTT requires all NTT employees to complete data privacy and protection training periodically. All data privacy and protection policies, processes, standards and guidelines are available to employees and communicated regularly. Where required, local, regional or functional training to support NTT employees to act in line with the requirements in specific countries, regions or business functions.

10. Security for privacy

10.1 Taking into account the state of the art, cost of implementation and the nature, scope, context and purpose of processing personal data, as well as the risks to the rights and freedoms of data subjects; NTT has implemented appropriate technical and organizational measures to ensure the confidentiality, integrity, and availability of personal data.

10.2 NTT's security methodologies are aligned to ISO 27001 and the NIST Cyber Security Framework ('CSF').

11. Breach response and notification

11.1 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.

11.2 NTT is committed to ensuring that applicable data protection authorities, affected clients and affected data subjects are notified in the event of a personal data breach in compliance with applicable data protection laws and any contractual commitments.

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

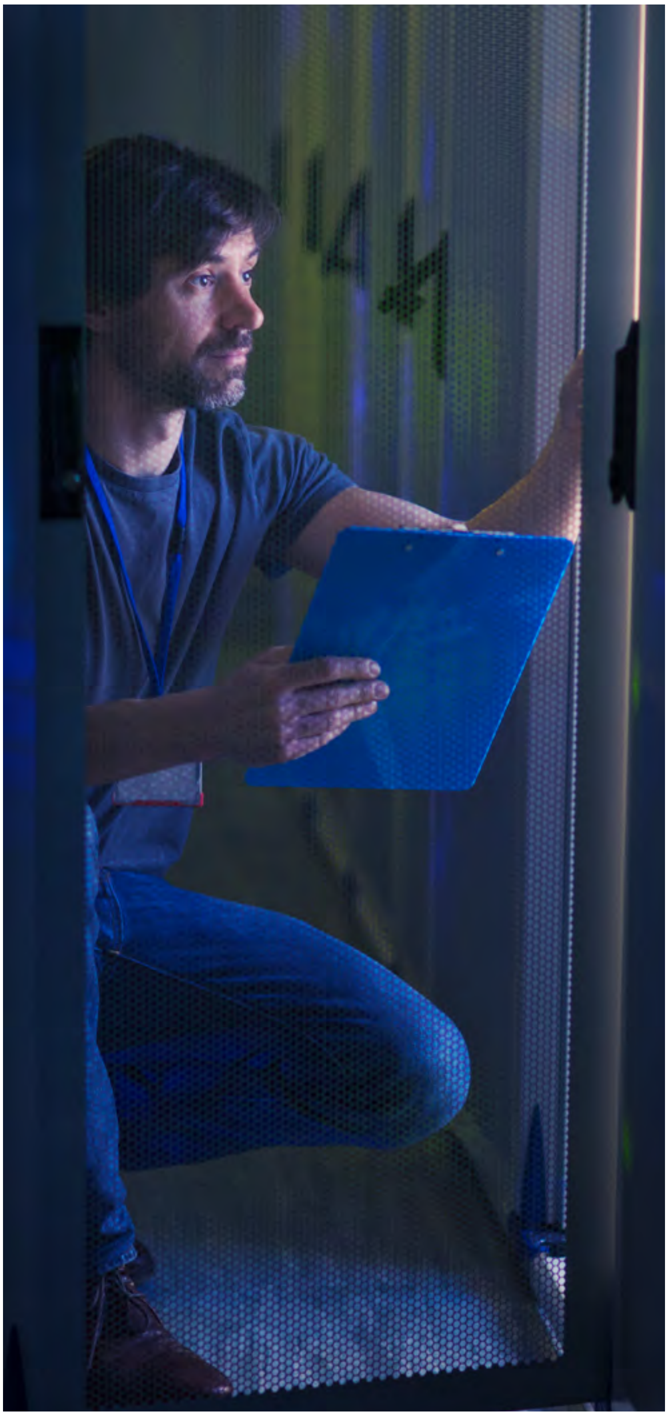
11.4 NTT incident management measures to identify, detect, respond and recover from information security incidents are outlined in Section B below of these TOMs.

12. Third party management

12.1 NTT is accountable for the actions of its processors and sub-processors who process personal data on NTT's behalf. NTT assesses the ability of its processors and sub-processors to protect personal data in accordance with NTT standards at the time of selection and periodically thereafter.

12.2 NTT processors and subprocessors are required to sign appropriate agreements that govern the processing and protection of personal data. These agreements include requirements to ensure that the same obligations are passed to any further processors who may process personal data.

B. Information security measures



NTT is committed to ensuring that information security is implemented and properly managed to protect the confidentiality, integrity and availability of personal data.

NTT has established a group-wide Information Security Management System ('ISMS') which holds an ISO 27001 certification.

13. Information security roles and responsibilities

13.1 Roles and responsibilities for information security have been formally assigned, with reporting lines that ensure the independence of the function, including a Chief Information Security Officer and Information Security Officers throughout the business functions.

13.2 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.

14. Information security policies

14.1 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.

15. Mobile device management

15.1 NTT has a Mobile Devices and Teleworking Policy. 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 corporate networks and client information, systems, networks and infrastructure.

16. Human resources

16.1 NTT has a Human Resources Policy. 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.

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

16.3 NTT employees are required to complete information security awareness training on an annual basis. Information security policies and supporting procedures, processes and guidelines are available to employees and communicated regularly.

16.4 NTT employees receive relevant information about trends, threats and best practices through NTT communication platforms.

17. Workplace surveillance

17.1 NTT implemented a workplace surveillance policy to implement processes and systems to protect and safeguard the Confidentiality, Integrity and Availability ('CIA') of all critical information (including Personal Data) and information processing assets.

17.2 The purpose of the Workplace Surveillance Policy is to inform NTT Users and others when workplace surveillance may take place.

17.3 NTT may conduct electronic monitoring and surveillance of Users in the place where the employee works, whether at a place of work provided by NTT, at a client or at home ('workplace') to protect against User misconduct, manage productivity, and increase workplace safety ('workplace surveillance').

18. Acceptable use

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

19. Asset management and classification

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

20. Access controls

20.1 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 principles of least privilege.

20.2 Where reasonable, NTT has applied industry-standard encryption at-rest and intransit to ensure that personal data is protected against any unauthorized access or disclosure. Access reviews are periodically performed on IT assets, applications, systems, and databases to ensure only authorized individuals have access.

20.3 NTT has undertaken reasonable efforts to strictly limit the number of privileged ('Admin') users on all applications, systems and databases and does not permit generic accounts or the sharing of credentials unless expressly authorized by management or NTT clients.

21. Encryption and key management policy

21.1 NTT has an Encryption and Key Management Policy that supports the efficient use of encryption and encryption key management within NTT to prevent unauthorized or malicious third parties from recovering the original information whether in transit or at rest. Associated standards provide guidance in the use of cryptographic controls for the protection of information.

22. Network security

22.1 NTT has a Network Security Policy containing measures that apply to NTT networks to manage, control and protect NTT information.

23. Application security

23.1 NTT has an Application Security Policy requiring that all NTT software applications developed in-house or purchased are managed, and access to these is controlled to protect NTT information as well as to ensure the in-house application development incorporates security best practices from the initial design stage of application development.

24. Backups

24.1 NTT has a Backup Policy that defines the requirements for maintaining and recovering backup copies of sensitive NTT information created, processed, or stored on NTT computers and communications systems.

25. System security policy

25.1 NTT has a System Security Policy requiring that NTT systems are managed and controlled to protect NTT information. NTT systems consist of all physical virtual systems, including servers, workstations and devices within the NTT corporate offices and the NTT Cloud.

26. Physical and environmental security

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

a. Physical access controls;
b. Monitoring and auditing of physical access;
c. Protection from environmental hazards;
d. Securing physical assets;
e. Cabling security;
f. Handling of physical assets;
g. Maintenance and disposal of physical assets;
h. Clear desk and screen practices;
i. Visitors access and supervision; and
j. Health and safety procedures.

27. Operational security

27.1 The NTT Digital & Global Business Services (‘DGBS’) Division is responsible for managing NTT applications, systems, databases and infrastructure in line with NTT Information Security Policies, Standards and Guidelines. DGBS documents, maintains and implements all IT operational policies, processes and procedures aligned to COBIT and ITIL standards.

27.2 NTT has a policy and supporting procedures for secure architecture, design, operation, and maintenance to govern changes to our business processes, applications, systems, databases and infrastructure. NTT operates several governance structures to review and approve changes based on the size and scope of the change and strategic objectives. All requests and their outcomes are logged and documented.

27.3 NTT has a Vulnerability Management Policy and 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.

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

27.5 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 backup issues, exceptions or failures.

27.5 NTT has an Information Security Monitoring Policy and 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.

28. System acquisition, development and maintenance

28.1 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.

28.2 NTT has undertaken reasonable measures to prevent the creation or maintenance of backdoors or similar programming that facilitate unauthorized access to or authorities to access personal data or NTT systems.

29. Third party management

29.1 NTT has a third-party Information 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 data privacy, information security due diligence and information security risk assessments to be performed, to ensure:

a. Information security requirements are clearly articulated and documented in agreements in accordance with NTT's information security standards.
b. NTT service providers and processors implement the same level of protection and control as NTT;
c. Service providers and processors are required to report any suspected or actual information security incidents to NTT promptly.

30. Information security incident management

30.1 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.

30.2 NTT has established groupwide 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.

31. Business continuity

31.1 NTT has established business continuity and disaster recovery plans. NTT has adopted a layered approach to ensure the availability of our systems and data.

32. Compliance

32.1 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.

NTT DATA