Technical and organizational measures

Data privacy and protection

Contents

Introduction

From strategic consulting to leading-edge technologies, NTT DATA enables experiences that transform organizations for success, disrupt industries for good and shape a better society for all.

Our technical and organizational measures describe how we ensure the protection of personal data in a transparent, fair, ethical and lawful way. They 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.

If you have any questions about these technical and organizational measures or how they relate to our products, services and solutions, please contact your service representative.

Our technical and organizational measures describe how we ensure the protection of personal data in a transparent, fair, ethical and lawful way.

Data privacy and protection measures

2.1. Governance and operating model

NTT DATA is committed to demonstrating accountability when processing personal data. We have the appropriate organizational structures, roles and responsibilities for managing and providing oversight of the processing of personal data.

In each jurisdiction where we operate, organizational units are required to dedicate appropriate resources to comply with applicable data protection laws. This includes appointing skilled data privacy resources to oversee compliance, as well as establishing appropriate reporting structures.

NTT DATA reports on the design and operating effectiveness of data privacy and protection activities to senior management on a periodic basis.

2.2. Policies, processes and guidelines

NTT DATA has implemented and communicated its policies, processes, standards and guidelines that detail how NTT DATA employees are expected to process personal data.

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

NTT DATA has implemented processes and templates for performing risk assessments, including data protection impact assessments (DPIAs), legitimate interest assessments (LIAs) and transfer risk assessments, in accordance with applicable data protection laws.

2.3. Data protection by design

NTT DATA 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 DATA products, services and solutions.

2.4. Data landscape

NTT DATA has implemented processes to identify, record, assess and understand the personal data that it processes.

NTT DATA maintains a record of the personal data processed in accordance with applicable data protection laws.

2.5. Information lifecycle management

NTT DATA 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).

NTT DATA maintains data retention policies and schedules, which are aligned to applicable laws. NTT DATA retains personal data only where there is a legitimate business reason for doing so, and in accordance with its obligations under law. NTT DATA destroys, deletes or deidentifies personal data when the retention period lapses and there is no legitimate business interest to retain the personal data for a longer period.

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

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

2.6. Data subject rights

Data protection laws in certain countries provide data subjects with specific rights in relation to their personal data. NTT DATA is committed to upholding these rights and responding to data subject requests in a timely, transparent, fair, ethical and lawful way.

NTT DATA has implemented appropriate policies and procedures to uphold the data subject rights in accordance with applicable data protection laws.

NTT DATA supports the following data subject rights:

- Right to be informed
- Right of access
- Right to rectification
- Right to be forgotten
- Right to data portability
- Right to restrict use
- Right to object (including the right to opt-out of direct marketing and the sale of personal data)
- Right to challenge automated decisions
- Right to nondiscrimination
- Right to complain

NTT DATA ensures appropriate channels are available to data subjects so they can exercise their rights in relation to personal data that NTT DATA may process about them.

NTT DATA maintains a record of all data subject requests received and the actions taken in response to these requests.

NTT DATA will provide all reasonable support to clients in responding to data subject requests, in accordance with existing agreements.

NTT DATA has established policies and procedures for responding to requests from public authorities to access personal data in accordance with applicable laws and contractual requirements. NTT DATA maintains a record of these requests and their outcomes.

2.7. Cross-border transfers

NTT DATA establishes appropriate safeguards (such as adequacy decisions, standard contractual clauses and other tools set out in applicable legislation) when engaging in cross-border data transfers.

When personal data is transferred across borders, NTT DATA performs transfer impact assessments (TIAs) to ensure the destination country offers an equivalent level of protection to the rights and freedoms of data subjects as the country where data was originally collected. Where such equivalence does not exist, we will assess and adopt supplementary measures to support data subject rights in accordance with our policies and legislative requirements. Where such supplementary measures cannot be implemented, NTT DATA will cease the transfer of personal data.

NTT DATA relies on standard contractual clauses to support the lawful transfer of personal data outside the country where it was originally collected. To support such transfers, appropriate agreements are in place with NTT DATA subsidiaries, group companies, affiliates, processors, subprocessors, and clients.

2.8. Regulatory

NTT DATA monitors changes to data protection laws in the countries in which it operates and has implemented processes and tools to support compliance.

2.9. Training and awareness

NTT DATA is committed to implementing a culture of awareness and compliance through ongoing training and awareness initiatives. We require all employees to complete mandatory data privacy and protection training on a periodic basis. Training materials and related policies, processes, standards and guidelines are available to employees and communicated regularly. Where required, local, regional or functional training is provided to support employees to act in line with the requirements in specific countries, regions or business functions.

2.10. Security for privacy

NTT DATA has implemented appropriate technical and organizational measures to ensure the confidentiality, integrity and availability of personal data, 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 DATA's security methodologies are aligned to ISO 27001 and the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF).

2.11. Breach response and notification

NTT DATA has policies, processes and procedures for identifying, detecting, responding to and recovering from a personal data breach, as well as for notifying appropriate stakeholders in the event of such a breach. These include mechanisms for performing a root cause analysis and undertaking corrective actions.

NTT DATA 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.

NTT DATA maintains a record of all personal data breaches and the actions taken in response to these events.

Section 3: Information security measures outlines our incident management measures to identify, detect, respond and recover from information security incidents.

2.12. Third party management

NTT DATA is accountable for the actions of processors and subprocessors who process personal data on our behalf. We assess the ability of these processors and subprocessors to protect personal data in accordance with NTT DATA standards at the time of selection and on a periodic basis thereafter.

NTT DATA 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 other processors who may process personal data.

Information security measures

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

NTT DATA has established appropriate policies, processes, procedures, standards and guidelines to ensure the security of data that it processes. NTT DATA's security methodologies are aligned to ISO 27001 as well as other industry best practices.

3.1. Information security roles and responsibilities

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

NTT DATA employees are responsible for acting in accordance with our information security policies, processes, standards and guidelines in their day-to-day business activities.

3.2. Information security policies

NTT DATA has documented and published a set of information security policies. These policies and supporting documentation are reviewed periodically.

3.3. Mobile device management

NTT DATA has established a zero trust architecture framework to implement and maintain security controls to access and interact with NTT DATA systems and information assets. This framework includes:

- End-user device management (EDM) policies and supporting procedures.
- Controls and tools to maintain the security.
- Confidentiality, availability and integrity of enterprise data. This data could be housed in or accessible via endpoint user devices (including mobile phones, tablets and devices allowing remote access).

3.4. Human resources

NTT DATA performs background and employment screening for its employees, to the extent permitted under applicable law, to validate their suitability for hiring, and for 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.

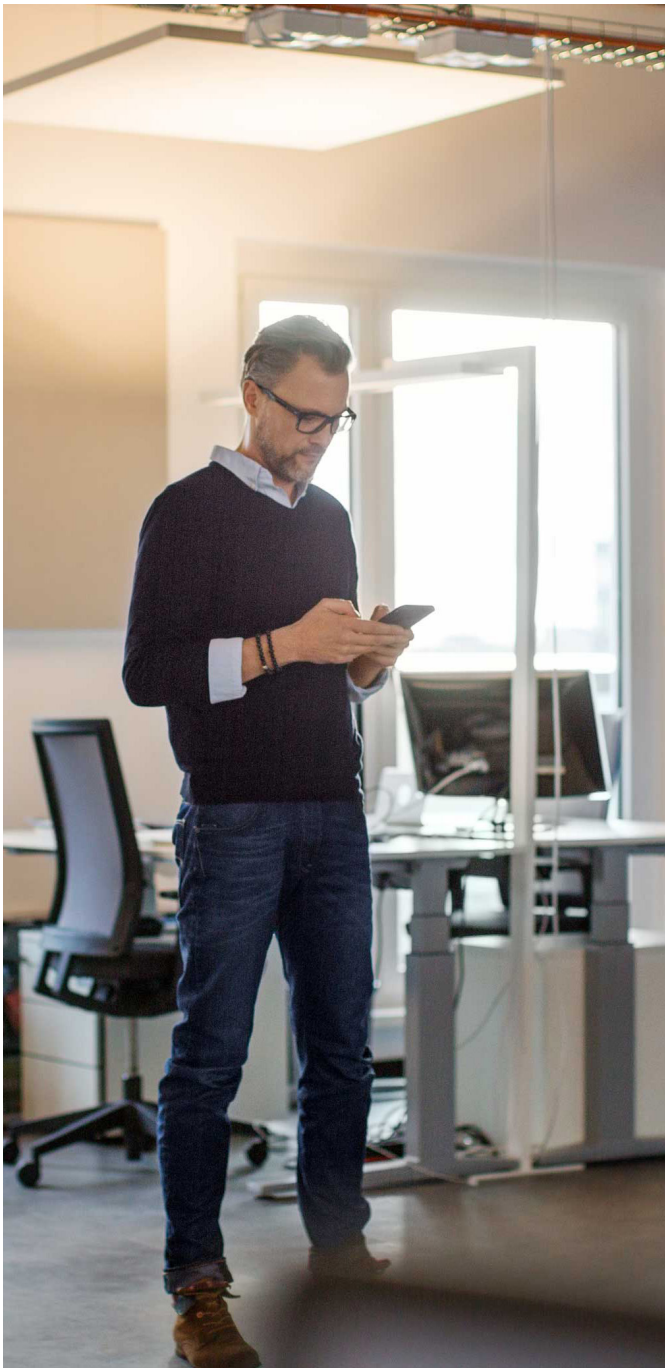
NTT DATA requires that all employees (including contractors and temporary employees) agree to maintain the confidentiality of company and client data (including personal data).

NTT DATA employees are required to complete information security awareness training and periodic refresher training. Information security policies and supporting procedures, processes and guidelines are made available to employees. Employees also receive relevant information about trends, threats and best practices. Security awareness campaigns are run periodically to ensure continued awareness.

3.5. Acceptable use

NTT DATA has established policies that support the proper and effective use of our information assets, which include computer and telecommunications resources, products, services, solutions and IT infrastructure.

NTT DATA has established information classification policies to support appropriate controls for handling information based on its classification. Information and assets are protected in line with the classification label.



> “NTT DATA’s security methodologies are aligned to ISO 27001 as well as other industry best practices.”

3.6. Access controls

NTT DATA has established access control policies, 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.

Where applicable, NTT DATA has applied industry-standard encryption at rest and in transit to ensure that personal data is protected against any unauthorized access or disclosure.

Access reviews are periodically performed to ensure only authorized individuals have access to NTT DATA systems and information assets.

NTT DATA has undertaken reasonable efforts to limit the number of users who have privileged access to NTT DATA systems and information assets.

NTT DATA does not permit sharing of accounts or credentials unless this has been approved through the relevant exception management process.

3.7. Asset management and classification

NTT DATA has established policies which govern the classification and handling of physical and informational assets, including the secure disposal of assets, to ensure that the information is protected at the appropriate level.

Assets are based on business criticality to determine confidentiality requirements. Industry guidance for handling personal data provides the framework for technical, organizational and physical safeguards. These safeguards may include controls such as access management, encryption, logging and monitoring, and data destruction.

3.8. Physical and environmental security

NTT DATA has implemented reasonable and appropriate measures in line with our physical security policies to prevent unauthorized physical access or damage to, or interference with information, applications, systems, databases and infrastructure. These include:

- Physical access controls
- Monitoring and auditing of physical access
- Protection from environmental hazards
- Securing physical assets
- Handling of physical assets
- Maintenance and disposal of physical assets
- Clear desk and screen practices
- Visitors access and supervision

3.9. Operational security

NTT DATA has established appropriate specialist teams who are responsible for managing and protecting NTT DATA's information systems and infrastructure.

NTT DATA has established policies and supporting procedures for managing changes to business processes, information systems and infrastructure. NTT DATA 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.

NTT DATA has established threat and vulnerability management programs, 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 antivirus and antimalware tools, regular scanning of environments, patching protocols, and the management of remediation and improvement activities.

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

System availability includes architecture, high-availability design, disaster recovery, 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 backups, is determined by NTT DATA business requirements, including client requirements, and the criticality of the information. Disaster recovery plans are tested periodically. Backup processes are monitored to ensure the successful completion of backups, as well as manage any backup issues, exceptions or failures.

NTT DATA applies 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.

3.10. System acquisition, development and maintenance

NTT DATA has established a zero trust architecture framework to govern the design, acquisition, development and maintenance of information systems and architecture.

Architecture and design policies and supporting standards and procedures exist to ensure that security-by-design principles are applied within the software development lifecycle.

3.11. Third party management

NTT DATA has established policies and practices for third party management to ensure that information assets are protected when NTT DATA engages third party service providers and/or processors. These include requirements for information security due diligence and information security risk assessments to be performed to ensure that:

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

3.12. Information security incident management

NTT DATA has policies, processes and procedures for identifying, detecting, responding to and recovering from an information security incident, including personal data breaches, and notifying appropriate stakeholders in the event of such an incident. These include mechanisms for performing a root cause analysis and undertaking corrective actions to remediate and prevent a reoccurrence.

NTT DATA has established enterprise-wide security operations to proactively monitor and manage all network and computing assets. These operations are supported by technical tools for information security incident response and recovery.

3.13. Business continuity

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

3.14. Compliance

NTT DATA has established roles and responsibilities for identifying laws and regulations that affect our business operations. Responsibility for compliance with laws and regulations is established at a group and regional level to ensure NTT DATA meets global and local requirements.


NTT DATA