

Personal Information Protection and Privacy

Policy

With the rapid spread of smartphones and other electronic information devices and the progress in new, AI-enabled services and innovations, concern with respect to the protection of personal information and privacy has markedly increased. Concern is particularly pronounced among the public in Europe, where the Charter of Fundamental Rights of the European Union (EU) has established protection of personal information as a fundamental right. The EU's General Data Protection Regulation (GDPR), which became effective in May 2018, stipulates methods of protection and management of personal information to protect and establish personal information and privacy rights.

Failure to consider these issues would be a serious risk for NEC as it seeks to provide social values such as safety, security, fairness, and efficiency through its services and solutions. On the other hand, by providing services and solutions that consider these issues we believe we can provide highly reliable value to society, including our customers.

The NEC Group Code of Conduct stipulates respect for human rights and privacy and the management of personal information, and NEC has positioned "Provision and Utilization of AI with Respect for Human Rights (AI and Human Rights)," including personal information protection initiatives, as a priority management theme from an ESG perspective—materiality.

We have studied the trends related to this framework of new laws and regulations, and we are addressing these problems regarding personal information protection or privacy by following the policies described below.

● Personal Information Protection

Personal information refers to personally identifiable information, which includes numbers and other identifiers, and we recognize that appropriately protecting personal numbers and other personal information

received from shareholders, investors, business partners, employees, and others is one of our social responsibilities. We have implemented and maintain the NEC Privacy Policy, which stipulates that personal information must be handled in conformance with Japan's Act on the Protection of Personal Information and JIS Q 15001 (Personal information protection management systems—requirements), the Japanese industrial standard for safe and appropriate management of personal information handled by corporations and other organizations in the course of their operations. In the event that the Company's policy should change, we will promptly give notice on the Company's public website and to all of our employees, in accordance with JIS Q 15001.

In cooperation with its consolidated subsidiaries throughout the world, NEC Corporation has built a system for promoting privacy protection and a personal information protection management system in compliance with the Act on the Protection of Personal Information and JIS Q 15001.

Our personal information protection management system includes the establishment of data protection standards (personal data safety management measures and so on). Further, we conclude agreements with those whom we share data requiring compliance with these standards. Also, we have established escalation rules and emergency response procedures to be followed in the event of incidents such as personal information leaks.

● Privacy

NEC Corporation acquired "PrivacyMark" certification in October 2005 and subsequently renewed it in October 2019. The PrivacyMark is conferred on companies that comply with JIS Q 15001 and are recognized by a third-party organization as having systems in place to ensure appropriate protection measures for personal information.

As of the end of March 2021, NEC Corporation and its 30 affiliated companies have obtained this certification. In principle, we forbid

acquiring information that could have an economic impact such as bank account or credit card numbers, sensitive information such as birthplace, or highly private information such as mobile telephone numbers without the person's consent.

The GDPR is one example of the global trend toward the establishment of privacy protection laws, and the roles and responsibilities required of companies have been increasing. NEC Corporation aims to maximize social value as well as to minimize the negative impact on society by developing and providing products and services that consider privacy issues, which can be perceived differently depending on country, region or culture, and human rights issues such as discrimination that may be exacerbated by leveraging AI.


To clarify our stance, in April 2019, we formulated and announced the "NEC Group AI and Human Rights Principles." The Companywide principles will guide our employees to recognize respect for human rights as the highest priority in each and every stage of our business operations in relation to AI utilization and enable them to take action accordingly.

In addition, the NEC Group Code of Conduct also stipulates that business activities aimed at resolving social issues by using ICT must not give rise to human rights issues, including invasion of privacy.

 [Respecting Human Rights](#)

 [AI and Human Rights](#)

 [NEC Privacy Policy](#)

 [NEC Group AI and Human Rights Principles](#)



Implementation Framework

At NEC Corporation, the head of the division responsible for protecting personal information serves as the Personal Information Protection Administrator, the person in charge of implementing the personal information protection management system. Further, we have added the role of protecting specific information with respect to the Social Security and Tax Number System to the duties of the Personal Information Protection Administrator.

The Customer Information Security Office of the Compliance Division plays a central part in promoting the protection of personal information within the NEC Group under the leadership of the head of the Personal Information Protection Promotion Bureau appointed by the Personal Information Protection Administrator.

In addition, we conduct regular audits of privacy protection in conformance with JIS Q 15001, with the General Manager of the Corporate Auditing Bureau serving as Chief Personal Information Protection Auditor.

The general managers are responsible for managing personal information protection in their respective divisions. Each appoints a division personal information protection manager, who is responsible for carrying out personal information protection management for the division, and a personal information protection professional, who possesses expert insight regarding protection of personal information. The manager operates a personal information protection management system by inspecting personal information, including human rights and privacy issues, and through personal information handling in each division and improving handling rules based on the inspection results. The person responsible for handling personal information for each project ensures that persons who handle personal information undertake thorough personal information protection measures.

● Consolidated Subsidiary Management Framework

At our consolidated subsidiaries in Japan, we have built systems to comply with the Act on the Protection of Personal Information and the so-called My Number Act, which is designed to centrally manage information related to social security and tax by assigning a number to individual citizens of Japan. At our consolidated subsidiaries abroad, we naturally comply with the laws in each country, and we have appointed

a Personal Data Administrator at each of our major subsidiaries to promote protection of personal information.

● Emergency Response to Information Leaks

NEC maintains systems pursuant to JIS Q 15001 for responding swiftly if an incident occurs involving the loss, outflow or leak, etc., of personal information. If an incident should occur, the response is coordinated quickly and systematically based on standardized procedures. Specifically, if an incident occurs related to personal information or an event takes place for which the occurrence of such an incident is a possibility, the discoverer or the employee involved in the incident contacts their manager and the NEC Group contact window for information security incidents. The person at that contact window then coordinates the necessary response with the related divisions that make up the Personal Information Protection Promotion Bureau and relevant divisions in accordance with applicable laws, ordinances, ministry guidelines, and other regulations, taking into account the risk for infringing on the rights and interests of the persons involved. These responses may include promptly notifying the people concerned, making a public announcement, and taking corrective measures appropriate to the incident.

● Response to Requests from National Governments for Personal Information Provision

If NEC Corporation's business divisions are requested by the governments or law enforcement agencies of countries to provide personal information that the Company holds, the general manager of the division that receives the request reports to and consults with the Personal Information Protection Administrator as necessary. In such cases, the Personal Information Protection Administrator reports to and consults with the executive officer in charge of personal information protection and management. Premised upon respect for the human rights of the person in question, appropriate measures are taken pursuant to the applicable laws.

In providing personal information in accordance with a request from a country's government or law enforcement agency, in principle, the Company obtains prior consent from the person in question and keeps a record of the provision. However, in some cases, pursuant to the laws and regulations of the country in question, consent is not obtained or a record is not kept of the provision. In the unlikely event that the provision

of personal information to the government or law enforcement agency of a country leads to an infringement of the human rights of the subject of said personal information, appropriate measures shall be taken pursuant to the applicable laws and regulations.

Further, given the legislative intent of the laws and regulations in each country, NEC does not publicly announce the number of requests for the provision of personal information that it receives from governments.

Measures and Main Fiscal 2021 Activities

● Training for Personal Information Protection

NEC Corporation conducts the following training for each management level in the organization.

Training for All Officers and Employees of NEC Corporation

Web-based training on information security, including the protection of human rights and privacy in relation to the protection and handling of personal information, is held online once a year for officers and employees of NEC Corporation. In fiscal 2021, the completion rate was 98%.

Education for Personal Information Protection Professionals (for the Company)

For the personal information protection professionals of all business divisions, the Company prepared a textbook on risk management in the handling of personal information—including the protection of human rights and privacy in relation to the handling of personal information—and conducted education through classroom lectures (16 lectures). At the same time, the Company conducted practical education based on the assignment submission method (three times).

Training for Newly Hired Employees and Transferred Employees of NEC Corporation and Its Consolidated Subsidiaries in Japan

In fiscal 2021, we created a textbook on personal information protection as introductory training material and used it in the training of newly hired and transferred employees. Apart from this training, when there is a request from a business division, or when it is otherwise deemed necessary by the Personal Information Protection Promotion Bureau, awareness training is conducted as appropriate at divisions or consolidated subsidiaries in Japan.

● Management of Personal Information

Initiatives at NEC Corporation

NEC Corporation runs the Personal Identifiable Information Control System, a ledger-based system to manage personal information and make its management more transparent.

Furthermore, we have documented standard procedures and operate a personal information protection management system. Also, as necessary, operational rules are created at the division level and by type of personal information and are rigorously enforced.

In addition, in order to raise awareness of personal information protection and information security in general, the Basic Rules for Handling Customer-related Work and Trade Secrets have been established, and NEC Corporation rigorously informs all employees about these rules.

As a result of these efforts, there were no incidents involving the loss, outflow or leak, etc., of personal information at NEC in fiscal 2021. There were also no complaints from the Ministry of Economy, Trade and Industry, which oversees the industrial area where NEC operates, the Personal Information Protection Commission, or from any other third-party institutions about customer privacy breach or other issues.

Initiatives for Customers and Business Partners

With respect to their contractors that handle personal information, NEC Corporation and its consolidated subsidiaries in Japan establish data protection standards (personal data safety management measures and so on), conclude agreements with contractors with which data is shared requiring compliance with these standards, and require contractors to conduct privacy management equivalent to that of the NEC Group. Moreover, we request the contractors engaged in work for NEC Corporation or its consolidated subsidiaries in Japan to submit a pledge on the Basic Rules for Customer-Related Work and to have their employees take a regular online test to verify their knowledge. These steps help ensure rigorous management of personal information.

As a result of these efforts, in fiscal 2021 there were no incidents involving the loss, outflow or leak, etc., of personal information. An “My Number” is Specific Personal Information that must be handled carefully, and we are doing so with security ensured. We are carrying out initiatives to deploy technical measures to ensure secure operations by controlling access, blocking unauthorized external access, and preventing information leaks, etc., while maintaining sufficient privacy protection levels in each system.

👥 Information Security and Cyber Security

Personal Information Management Initiatives Abroad

Recently, countries around the world, such as in Europe, are making rigorous laws and regulations regarding personal information. In this situation, NEC is ensuring proper information management globally as it pursues worldwide development of personal information-related businesses, such as AI, big data, IoT, and face recognition. We appoint Personal Data Administrators at our consolidated subsidiaries abroad to create a global management framework. At the same time, we are creating personal information management ledgers at every company and ensuring that everyone understands the procedures for managing them and the common information security rules that need to be observed. With regard to the GDPR, our consolidated subsidiaries in Japan and Europe have formulated personal information management rules based on the regulations and have concluded transfer agreements throughout the entire Group to ensure that cross-border transfer of personal information of European employees and others is conducted legally. Further, with respect to the California Consumer Privacy Act (CCPA), which was enforced in January 2020, we support consolidated subsidiaries to which said act is applicable by providing required information and by other means. In other areas, we have confirmed the legal and regulatory situation in relevant countries, such as Brazil’s Lei Geral de Proteção de Dados (LGPD) (Brazilian General Data Protection Law) and Thailand’s Privacy Data Protection Act (PDPA), and we are making the necessary preparations to comply with them.

● Monitoring and Improvement

NEC Corporation appropriately manages personal information by executing plan do check act (PDCA) cycles on an autonomous basis through various inspection activities.

Also, NEC Corporation and its consolidated subsidiaries in Japan conduct regular internal audits based on internal audit check items stipulated in JIS Q 15001. Further, for operations related to the handling of My Numbers, we use security control measure check sheets prepared based on Japan’s security control regulations and self-check sheets during re-entrustment in order to monitor divisions and subcontractors handling My Numbers.

Verification of the Operation of Information Security Measures

At NEC Corporation, implementation of information security measures by individual employees is verified once a year, and if there are cases of noncompliance, improvement plans are formulated and carried out at the organization level.

Verification of Status of Personal Information Management

At NEC Corporation, control forms registered in the Personal Identifiable Information Control System are reviewed at least once a year to validate the status of management of the various types of personal information handled by each organization. Further, once a year the general managers of business divisions organize management reviews for the verification of personal information management in business divisions, take corrective action as required, and maintain an appropriate management situation.

Verification of Operations during Emergencies

Operation of the above information security measures is thoroughly reviewed and readjusted as the need arises, in the event of an incident involving the loss, outflow or leak, etc., of personal information.