RNA Group K.K., H&R Consultants K.K., and Relo Japan K.K. (hereinafter collectively referred to as "the Group") strive to ensure information security and protect the personal information of both customers, business partners, contractors, employees, etc. (hereinafter collectively referred to as "customers, etc.") and the Group's businesses.

If you have any questions about this privacy policy, please contact privacy@hrcjapan.com.

1. Objective
   1.1. The Group is committed to protecting the personal information that customers provide to the Group and complying with all applicable privacy laws and regulations. As part of this pledge, we are pleased to inform you how the Group handles such information.

2. Basis of privacy
   2.1. Personal information in this policy refers to "personal identifiable information" as defined by the National Institute of Standards and Technology (NIST). This definition includes any information that may be used to identify or track an individual's identity, or any other information that may be associated with or related to an individual, such as information about medical care, education, finances and employment.
   2.2. We have acquired ISO 27001:2022 certification (ISO 27001:2022 is an international standard for information security management that verifies the organization's ability to effectively apply the security framework to business processes that identify, manage, and reduce risks to information security in all areas of business and at all levels). On February 26, 2018, the Group's Information Security Management System (ISMS) was certified by Intertek, an external independent certification body, to conform to the requirements of ISO 27001.

3. Rights of customers
   3.1. Customers may request reports on personal information entrusted by the Group. Contact privacy@hrcjapan.com to request a report on your personal data.
   3.2. Upon request, the Group will delete the personal information of the customer, etc., except in cases where the Group is required to retain the personal information of the customer, etc., as described in Section 12.1. Please be aware that this requirement may not be able to complete these services if the services started by the customer are not completed.
   3.3. The Group's website provides links to this privacy policy in an easy-to-understand location in order to ensure that you understand the Group's commitment to the privacy of our customers and the options of our customers.

4. User information to be collected and the collection method
   4.1. Website
      4.1.1. The Group will not collect personal information from anyone who visits the Group's website, except when customers provide personal information through the Contact Form at their own discretion.
      4.1.2. Our website uses Cookie to understand the usage of our website. The collected data is analyzed by analytical software such as Jetpack and Google Analytics installed on the Group's website and is used to obtain information such as the number and use of customers. This collected information does not include any information that can identify individuals. Please refer to our Cookie policy: https://hrcjapan.com/en/cookie-policy/

4.1.3. The Group may provide links to third-party websites, products and services for information purposes only. These links are not authorized or vetted by the Group. Please consider or assume that these third parties do not know about or agree to comply with the Group's privacy policies when deciding whether to visit/click on them.

4.2. Data Collection

4.2.1. The Group collects personal information based on the "minimum necessary" principle. We will collect, use, and maintain only the personal information necessary to implement the services requested by our customers.

4.2.2. The Group may require the following personal information to perform the requested services: Name, date of birth, passport number, current address, mail address, postal address, telephone number, bank account information, credit card information, employment contract information, visa information, etc.

4.2.3. The Group collects TLS-encrypted Microsoft Office 365 emails and SSL-encrypted information needed to provide services through a file transfer system that has the ability to download files, identify downloaders, and create output audit logs. Other collection methods include portal sites for relocation management companies, personnel representatives from business partners, direct interviews, telephone and fax, and interactions with the Group's website and tools.

5. Purpose of Use

5.1. The Group will use personal information under the "minimum necessary" principle. We will collect, use and maintain only the personal information necessary to perform services initiated by customers as part of these services.

5.2. The Group may also use personal information for internal purposes, such as audits, data analysis, training and research, to improve the Group's products, services and communications.

5.3. Without the use of personal information, the Group may use personal information in urgent situations that could lead to imminent threats to human life and public safety.

5.4. The Group may use personal information in special circumstances to comply with legitimate requests from law enforcement agencies or to conduct internal investigations of fraudulent activities.

5.5. Personal information received from customers is collected only for business purposes and activities. This includes, but is not limited to, the following:

- In order to perform services requested by customers
- For billing purposes
- To provide the Group's services to customers, etc.
- To maintain the details of transaction information
- To provide information on the Group's products and services when requested
- To conduct customer satisfaction surveys and arrange for the Group's information, services or products with the aim of improving and strengthening the products and services provided to customers, etc.
- To raise brand awareness, provide information on Japan lifestyles to customers, etc., and inform customers of products and services they are interested in

6. Shared use

6.1. The Group may be used jointly by the Group to the extent necessary to achieve the above purpose of use.

7. Provision to a Third Party
    7.1. The Group may provide personal information obtained to third parties with the consent of the customer, etc., if necessary to achieve the objectives of the business and maintain its activities.
    7.2. In rare cases, the Group is required to disclose personal information to law enforcement agencies, government agencies, or external advisors. The Group will make these disclosures in accordance with all applicable laws and regulations.

8. Matters Specific to Insurance Services (Provided by a Third Party)
    8.1. Group company H&R Consultants K.K. operates insurance agencies and real estate agencies. Personal information collected at the time of provision of real estate services is shared to process the application for insurance contracts only when the service is started by the customer, etc.
    8.2. Personal information that you share with each partner's insurance company is used to provide services in a variety of ways. Individual policies can be viewed on each partner's website.
        8.2.1. H&R Consultants K.K. may conduct business transactions with the following companies and share the above information.
            - Chubb Insurance Japan (https:/www.chubb.com/jp-jp/)
            - Tokio Marine & Nichido Fire Insurance Co., Ltd. (https:/www.tokiomarine-nichido.co.jp/)
            - Housing Indemnity, Ltd. (http://www.kyousaikai.co.jp/)

9. Staff training
    9.1. We ensure that our staff understand the procedures and follow the procedures when dealing with personal information related to regulatory standards and privacy policies, and provide the following training:
        9.1.1. Periodic training to ensure that all staff systematically protect both customers and companies' information assets and familiarize themselves with the requirements of the Group's Information Security Management System (ISMS) based on ISO/IEC 27001:2022
        9.1.2. Regular training on encryption best practices
        9.1.3. Regular training on the best practices for password and password management systems described in our password policy

10. Data integrity
    10.1. The Group must maintain accurate data in order to perform services initiated by customers, etc., and will use all reasonable methods to ensure that the customer's personal information is accurate.

11. Data security, maintenance, and disposal
    11.1. The Group implements information security measures and uses industry best practices in operations, procedures, and measures to systematically protect personal information in custody from loss or unauthorized access, destruction, use, change, or disclosure.
    11.2. Data security

11.2.1. The data is stored in the Group's dedicated server hosted in Japan or in the Group's customer database hosted outside Japan. The Group restricts access to personal information in multiple ways.

11.2.2. Within our dedicated servers, we collect personal information in specific locations and maintain strict access restrictions through Active Directory authorities that apply access restrictions, separation of duties, and the principle of least privilege.

11.2.3.This dedicated server can only be accessed through an encrypted virtual private network (VPN) using a fixed IP address in our office. Authenticated users can access outside of the Group's office via a VPN client if necessary.

11.2.4. The Group's cloud servers hosting the customer database have fixed IP addresses for the Group Office and are strictly controlled and maintained by access restrictions, separation of duties, and logins of users who apply the principle of least privilege assigned through the application. The application is built to comply with the best practices presented by OWASP, and it is SSL-encrypted. Authenticated users can access outside of the Group's office via a VPN client if necessary.

11.2.5. Our staff must use strong passwords for all logins in accordance with the provisions of our password policy.

11.2.6. All computers in the Group are secured through enterprise IT management tools that allow us to monitor events that may affect the confidentiality of personal information.

11.2.7. In the event of a security breach related to the loss of non-public information in the Group, the following actions will be taken.

- We will notify the impacted customers, etc.
- We will support affected customers in preventing or limiting the adverse effects of infringements.
- We will outline what measures have been taken to improve problems caused by infringement.

12. Security Control Measures

12.1. Data Retention

12.1.1. The Group shall apply the "minimum necessary" principle and retain personal information. We will collect, use and maintain personal information only to the extent necessary to maintain the Group's business objectives and activities as expected by our customers.

12.1.2. The following are the guidelines for customers' data held by the Group after the achievement of the objectives and after the completion of the activities. We retain the data necessary to comply with the Group's legal obligations.

12.2. Disposing of data

12.2.1.Unless personal information is required to be retained as described in 3.2 above, the Group shall dispose of such personal information that is no longer required for the performance of services initiated by customers, etc. on a standard schedule.

13. Change procedure

13.1. This policy is subject to review and revision without notice to continually improve the Group's ability to protect personal information and to reflect current laws. These changes will be published on this page, which contains our official privacy policy.

14. Disclosure of Personal Information
    14.1. The Group shall disclose personal information to customers and others without delay after confirming that it is a request from the person in question when requested by customers and others to disclose such information in accordance with the Personal Information Protection Law. This provision shall not apply to the cases where the Group is not obliged to disclose.

15. Correction and Suspension of Use of Personal Information, etc.
    15.1. In the event the Group is requested by customers, etc. to rectify the contents of personal information based on the provisions of the Personal Information Protection Law on the grounds that the personal information is not true, or is collected by deception or other wrongful means on the grounds that the personal information is handled beyond the scope of the purpose of use that has been publicly announced in advance, the Group shall conduct necessary investigation without delay after confirming that the request has been made by the customer, and based on the results of the investigation, the Group shall correct the contents of the personal information or suspend the use of the personal information and notify the customer, etc. to that effect. In the event the Company decides not to correct or suspend the use, the Company shall notify the Customer to that effect.
    15.2. In the event the Group determines that it is necessary for the Group to comply with a request for deletion of personal information of the Person in question, etc., the Group shall confirm that such request has been made by the Customer, delete such personal information, and notify the Customer, etc. thereof.
    15.3. The Act on the Protection of Personal Information and other laws and regulations shall not apply where the Group is not obliged to make corrections, etc. or suspend use, etc.

16. Inquiry desk
    16.1. We request you to ask questions and inquire about our personal information practices and our privacy policy.

RNA Group K.K.
Information security manager
〒460-0002 4F Nakato Marunouchi Bldg., 3-17-6, Marunouchi, Naka-ku, Nagoya
TEL 052-973-3957 FAX 052-973-9293
E-mail: privacy@hrcjapan.com

Japan's Personal Information Protection Law (amended Personal Information Protection Law, which entered into force on April 1, 2022)