

DATA PRIVACY AND COLLECTION NOTICE

We, The Reynolds Company (hereinafter referred to as “the Company”), have adopted this Data Privacy and Collection Notice to inform you of our privacy practices. This statement sets forth our policies and practices for handling the information we collect and use in the employment context.¹

Information We Collect

We collect personal information of employees, job applicants, independent contractors, and their respective emergency contacts and dependents, including:

- **Identifiers** such as name, address, telephone number, unique personal numbers (such as social security, insurance policy, bank account, and driver’s license numbers), passport data, signature, or other similar identifiers;
- **Professional or employment-related information** such as employment history, job performance evaluations, salary and other compensation information, benefits and allowances, tenure, hours worked, terms of employment, drug testing results, records of any disciplinary proceedings or investigations, job responsibilities, background check information, business and travel expenses, and documentation relating to immigration status;
- **Education information** such as transcripts, certifications, skills and proficiencies, and trainings attended;
- **Demographics** such as age, race, color, ancestry, national origin, citizenship, religion or creed, marital status, medical condition, physical or mental disability, sex (including gender, gender identity, gender expression, reproductive health, pregnancy or childbirth and related medical conditions), sexual orientation, veteran or military status, and genetic information (including familial genetic information);
- **Video recordings** of access to facilities;
- **Internet or other electronic network activity information** associated with use of Company-provided equipment, networks, or other resources, including but not limited to incoming and outgoing electronic communications, browsing history, search history, interactions with websites or applications, login credentials, electronic records and files, IP addresses and other information associated with network activities, and logs of application access and use. We also may collect information via cookies placed on Company websites with which you interact;
- **Information Specific to Rotational Staff** such as all professional or employment-related information including (i) employment, compensation or benefits collected and kept by ITOCHU Corporation or ITOCHU International Inc. (or other affiliates from which staff is dispatched), information related to application for visas and otherwise related to entry into and work permits in the United States, information related to tax returns, information related to all allowances, and all other information that is deemed relevant for the visa status or compliance with applicable internal rules and (ii) managing employment matters at ITOCHU Corporation or ITOCHU International Inc. (or other affiliates from which staff is dispatched), such as performance evaluation, appraisals, promotions, investigations and disciplinary actions in accordance with its internal rules, safety, health and welfare, administration of salaries, bonuses, pension plans, allowances and other compensations, and preparation and filing of tax returns²; and

¹ As required by applicable law, this notice applies to both Company employees and contractors. It does not change or otherwise affect workers’ classifications as employees or independent contractors.

² For the avoidance of doubt, this category of personal information only applies to Rotational only.

- **Other information, including health and safety information as relevant to employment** such as vaccination status and/or test results, including information of vaccination type, vaccination dates and locations, COVID-19 test methods, and when/where such tests results were obtained.

Sources of Information

We obtain the categories of personal information listed above from the following categories of sources:

- Directly and indirectly from our affiliates, employees, job applicants, contractors, customers, or their agents.
- Directly and indirectly from online activity on our company network.
- From business partners that interact with us in connection with the services we perform. For example, from vendors that support our hiring, employment, daily operations and/or the corporate network (e.g. background checks).

We may also collect other information directly and indirectly from various federal, state or local government sources, including for example from the judicial system (e.g., garnishment orders).

Use of Personal Information

We may process your personal information, including your sensitive personal information, for the following business purposes:

- **Workforce Management:** Managing work activities and personnel, such as recruitment, appraisals, performance management, promotions and succession planning, rehiring, administering salary, and compensation administration and reviews, wages, bonuses, and other awards, equity plan (such as stock options, stock grants, and employee stock purchase plan) participation and administration, processing accounts payable and receivable for employee healthcare benefits, pensions and savings plans, training, leave, managing disability and sickness leave, promotions, transfers, secondments, pension plans, honoring other contractual benefits, providing employment references, loans, performing workforce analysis and planning, performing employee surveys, performing background checks, managing disciplinary matters, grievances and terminations, reviewing employment decisions, making business travel arrangements, managing business expenses and reimbursements, planning and monitoring of training requirements and career development activities and skills, and creating and maintaining one or more internal employee directories.
- **Workforce Analytics:** We use workforce analytics for succession planning, workforce management, and data security. For instance, we use workforce analytics to assist in succession planning, to ensure business continuity, to design employee retention programs and diversity initiatives, to offer training opportunities and to identify patterns in the use of technology systems and to information entrusted to us, and to protect our associates and property.
- **Communications and Emergencies:** Facilitating communication with you, ensuring business continuity, managing company-owned property (e.g., laptops and mobile phones), providing references, protecting the health and safety of associates and others, safeguarding IT infrastructure, office equipment and other property, and facilitating communication with you and your nominated contacts in an emergency.
- **Business Operations:** Operating and managing the IT and communications systems (including email collection, storage and review), managing product and service development, improving products and services, managing company assets, allocating company assets and human resources, strategic planning, project management, business continuity, compiling audit trails and other reporting tools, maintaining

records relating to business activities, budgeting, financial management and reporting, communications, managing mergers, acquisitions, sales, re-organizations or disposals and integrating with purchasers.

- **Compliance:** Complying with legal and other requirements, such as income tax deductions, record-keeping and reporting obligations, conducting audits, complying with government inspections and other requests from government or other public authorities, responding to legal process such as subpoenas, pursuing legal rights and remedies, defending litigation and managing internal complaints or claims, conducting investigations, including employee reporting of allegations of wrongdoing, policy violations, fraud, and financial reporting concerns, and complying with internal policies and procedures.
- **Monitoring Use of Technology:** We collect information about the use of our information assets and resources, including internet access, electronic communications, and application usage. We collect this information to assess compliance with applicable laws and policies, to protect our resources against unauthorized access, and to prevent crime and fraud.

Disclosing Personal Information

We are committed to maintaining your trust, and we want you to understand when and to whom we may disclose the information (including the sensitive personal information) we collect.

We may disclose your personal information for a business purpose to the following categories of third parties:

- **Authorized third-party vendors and service providers.** We may share Identifiers, Professional or employment-related information, Education information, Demographics, Internet and other electronic network activity, Information Specific to Rotational Staff and Other information (as such categories are described in further detail above) with third-party vendors and service providers that provide services to us for a variety of business purposes, such as payment processing, email deployment, security and performance monitoring, maintaining or servicing accounts, data hosting, auditing, and data processing.
- **Corporate affiliates.** We may share Identifiers, Professional or employment-related information, Education Information, Demographics, Internet or other electronic network activity, Information Specific to Rotational Staff and Other information (as such categories are described in further detail above) with our corporate affiliates for a variety of business purposes, such as employee management, compliance, security and performance monitoring.
- **Business transfers.** We may share any personal information we collect in connection with a substantial corporate transaction, such as the sale of a website, a merger, consolidation, asset sale, initial public offering, or in the unlikely event of bankruptcy.
- **Legal purposes.** We may disclose all personal information we collect to (i) respond to subpoenas, court orders, legal process, law enforcement requests, legal claims or government inquiries, (ii) to protect and defend the rights, interests, safety, and security of the Company, our affiliates, users, or the public, and (iii) complete and file business registrations, licenses, permits, filings and other similar applications.
- **Customers.** We may share Identifiers, Professional or employment-related information, Education information and Demographics we collect to respond to customer business inquiries, such as customer registration processes or sanctions and compliance review.
- **With your consent.** We may share any personal information for any other purposes disclosed to you at the time we collect the information or pursuant to your consent.

We also may share your information with Company employees who need to know the information for the purposes described in this notice, including in the recruiting, human resources, legal and information technology departments.

In the preceding 12 months, the Company has not sold your information to third parties or shared it for purposes of cross-context behavioral advertising. The Company has not knowingly sold or shared the personal information of California residents who are younger than 16.

The Company does not use or disclose sensitive personal information beyond those purposes described above.

Data Retention

We retain your personal information for as long as needed for the above business purposes, to fulfill a legal obligation, for contractual purposes, and as otherwise permitted under applicable law.

Your Rights

You may be entitled, in accordance with applicable law, to the right to access your personal information in a portable format, delete your information, correct your information, or request more information about our information practices. If you become aware of changes or inaccuracies in your information, you should inform us of such changes so that the information may be updated or corrected. Requests should be submitted in writing as set out below. Once we receive your request, we may verify it by requesting information sufficient to confirm your identity.

You may be entitled, in accordance with applicable law, to submit a request through an authorized agent. To designate an authorized agent without power of attorney to exercise your rights and choices on your behalf, please provide your authorized agent with signed, written permission demonstrating that they have been authorized by you to act on your behalf and send such written permission to the Company's Human Resources department. If your authorized agent holds power of attorney, we may take reasonable steps to verify the request.

We will not discriminate against you for exercising your rights and choices, although some of the functionality and features of services offered to you by the Company may change or no longer be available to you.

Your rights may vary depending on your location and residence.

Security

We maintain reasonable security measures to safeguard information from loss, theft interference, misuse, unauthorized access, disclosure, alteration, or destruction. We also maintain reasonable procedures to help ensure that such data is reliable for its intended use and is accurate, complete, and current. You should understand that no data storage system or transmission of data over the Internet or any other public network can be guaranteed to be 100 percent secure, accurate, complete, or current. Please note that information collected by third parties may not have the same security protections as information you submit to us, and we are not responsible for protecting the security of such information.

Changes

This notice was last updated January 1, 2023. We may make changes to it from time to time to better clarify our practices and comply with applicable laws. Changes to this notice will be posted on the Company intranet.

Questions and Requests

If you have any questions or comments about this Data Privacy and Collection Notice, the ways in which we collect and use your personal information, or your choices and rights regarding such use, contact your Human Resources representative, your Compliance Officer or the Legal & Compliance Division at compliance@itochu.com. You may also access our Compliance Hotline at 844-269-9218, iii.ethicspoint.com, itochuinternational.ethicspoint.com, or via this QR code

