



PRIVACY POLICY AND NOTICE AT COLLECTION

Effective Date: 12/31/2024

Your privacy is very important to Dohrn Transfer Company and its operating groups, subsidiaries and affiliates (“Dohrn,” “we,” or “us”). Accordingly, we have developed this Privacy Policy and Notice at Collection (“Privacy Policy” or “Policy”) to describe how we collect, use, and disclose the personal information we collect from you through your use of our website, <https://www.dohrn.com> and through other online and offline methods. If you are a resident of Canada, please see the “Privacy Notice Addendum for Residents of Canada,” below.

This Policy does not address our processing of the personal information of our job applicants, employees, and independent contractors for human resources, employment, benefits administration, health and safety, and other similar business-related and legal compliance purposes. If your information pertains to one of the above-listed categories of individuals, please refer to our Privacy Notice and Notice at Collection for California Employees and Privacy Notice and Notice at Collection for California Job Applicants, as appropriate, for information about our collection, use, disclosure, and retention of your personal information. If you are our employee, we may collect your biometric information, and our collection, use, and disclosure of your biometric information will be governed by our Biometric Privacy Policy, which is publicly-available at <https://www.dohrn.com/privacy>. This Policy also does not apply to information that has been de-identified, aggregated, or is otherwise exempted from applicable data protection legislation.

Individuals with disabilities may access this Policy in an alternative format by contacting HumanResources@Dohrn.com or by calling 888-364-7621. Certain terms used in this Privacy Policy have the meanings given to them in the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act and implementing regulations (collectively the “CCPA”).

I. **Personal Information We Collect**

Depending on your interactions with us, we may not have collected each of these categories of personal information about you. However, we may collect (and may have collected during the 12-month period prior to the effective date of this Policy) the following categories of personal information about you:

- Identifiers, such as name, address, telephone number, or e-mail address, unique personal identifier (e.g., device identifier, unique pseudonym, or user alias/ID), online identifiers, account credentials, IP addresses, and other similar identifiers.

- Internet or other electronic network activity information, such as information about your device(s) when accessing our websites and your usage details of our websites, information you provide when filling in forms on our websites, the type of browser you use, the files you request, or information you provide when requesting further information, products, or services from us.
- Categories of personal information described in California Civil Code § 1798.80, such as name, signature, telephone number, financial information such as bank account number, credit card number or debit card number, or other financial information, state identification card number, and driver's license number.
- Professional and employment-related information, such as information relating to your position, (e.g., job title, job description, or department), employment status, employment history, or business email address.
- Commercial Information, such as records of products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.
- Geolocation data, such as time and physical location related to use of an internet website, application, device, or physical access to an office location.
- Sensory or surveillance information, such as video surveillance of our offices and other physical locations.
- Inferences and profiles based on other personal information, such as information about your behavior, preferences, characteristics, psychological trends, or predispositions.
- Other information you choose to provide.

We do not collect or process "sensitive personal information" (as defined by the CCPA) for the purpose of inferring characteristics about individuals.

Some internet browsers have a "Do Not Track" feature that lets you tell websites that you do not want to have your online activities tracked. Given that there is not a uniform way that browsers communicate the "Do Not Track" signal, our website does not currently interpret, respond to or alter its practices when it receives "Do Not Track" signals.

II. Sources of Personal Information

We collect and receive, and during the 12-month period prior to the effective date of this Privacy Policy, may have collected and received personal information from the following sources:

- Directly from you when you provide it to us;
- From third parties, such as our service providers and business partners; and
- Automatically and indirectly from you, such as through logging and analytics tools, cookies, pixel tags, and other similar technologies on our website.

III. Purposes for Using, Disclosing, and Otherwise Processing Personal Information

We may use, disclose, or otherwise process (and may have used, disclosed, or otherwise processed in the 12-month period prior to the effective date of this Policy) personal information for the following purposes:

- Providing our websites and supporting the features and contents available to you.
- Providing our products and services.
- Personalizing your digital experience with us, including enhancing features and designing relevant alerts, products, or services, and sending you marketing offers.
- To respond to your inquiries and supply you with requested information on our products and services.
- Understanding how you and others use our websites and to determine what features and services may interest you or our other customers.
- Operating and improving our organization and our services.
- Communicating with you and others, including responding to requests and inquiries, providing support, and providing promotional content.
- Troubleshooting, de-bugging, and otherwise addressing issues that may arise with the functionality of the websites.
- Helping to ensure security and integrity, to the extent the use of your personal information is reasonably necessary and proportionate for these purposes.
- Protecting the legal rights, property, safety, and security of records or information, our customers and website users, our organization and others, including detecting and preventing security incidents, fraud, misuse of the website, harassment, and other malicious, deceptive, unauthorized, or illegal activity.
- Complying with industry standards, applicable law, judicial process, any properly authorized civil, criminal, or government or regulatory investigation or request, or any subpoena or summons issued by a competent authority.
- Enforcing our policies, terms of use, or rights arising from contracts.
- For certain short-term transient uses.

In addition, we may also use, disclose, or otherwise process your personal information for purposes as you may authorize at the time you submit the information or as otherwise compatible with the above purposes or your reasonable expectations.

We may also de-identify personal information by removing any details that identify you personally. De-identified personal information will not be subject to this Policy and will be used to the extent permissible under applicable law.

IV. “Sales,” “Sharing,” and Disclosures of Personal Information for a Business Purpose

We do not:

- Sell your personal information;
- Share or disclose your personal information for cross-context behavioral advertising;

- Use your sensitive personal information for purposes other than those allowed by the CCPA as set out in cal. Code Regs. tit. 11 § 7027(m);
- Sell or share the personal information of individuals under 16 years of age as those terms are defined under the CCPA.

We generally disclose, and in the preceding 12 months we may have disclosed, the categories of personal information listed above in Personal Information We Collect to the following categories of entities for business or commercial purposes as described in Purposes for Using, Disclosing, and Otherwise Processing Personal Information, above:

1. To our subsidiaries and affiliates;
2. To our service providers we use to support our business, such as IT operating system and platform vendors, security vendors, monitoring and data analytics providers, and payment service providers; and
3. To other third parties, such as regulatory authorities or other third parties in response to legal process or other legal reporting requirements; to potential buyers (and their agents and advisors) in connection with any proposed merger, acquisition, or any form of sale or transfer of some or all of our stock or assets (including in the event of a reorganization, dissolution or liquidation); and to other similar third parties where disclosure is required for an ordinary business purpose in connection with our provision of services.

V. Retention of Personal Information

We will retain personal information as long as necessary for the fulfillment of the purposes described in this Privacy Policy, including but not limited to providing and administering the websites, providing you with customer service, answering your queries, complying with applicable laws, regulations, rules, and requests of relevant law enforcement and/or other governmental agencies, and protecting our, our employees', and our business partners' and customers' rights, property, or safety and the rights, property and safety of others. We may retain personal information for a longer period of time if a longer retention period is required or permitted by applicable law. In specific circumstances, we may also retain your personal information for longer periods of time so that we have an accurate record of your dealings with us in the event of any complaints or challenges.

VI. Confidentiality and Protection of Your Personal Information

We protect personal information by implementing appropriate physical, technical, and organizational safeguards designed to protect against loss or theft, as well as unauthorized access, disclosure, copying, use or modification. In addition, we take measures to limit access to personal information to those employees, agents, contractors, and other third parties that have a legitimate business need for such access. Although we use appropriate security measures once we have received your personal information, the transmission of information over the internet is never completely secure, so we cannot guarantee that your personal information will remain secure in all circumstances.

We use payment card processors during order processing. Your payment data is delivered directly from the browser to payment card processors, who handle your payment card data

subject to industry standards regarding security. It is important for you to protect against unauthorized access to your account, purchase history, and device. If you have created an account, please safeguard and do not share your credentials.

VII. **Third-Party Links**

We may provide links to other websites and services for your convenience, which are not subject to this Policy. The operators of the linked websites and services may have posted their own privacy policies that you should review to learn more about their privacy practices. If you decide to access any of the third-party websites linked to our websites, you do so entirely at your own risk and subject to the terms and conditions of use for such third-party websites.

HumanResources@Dohrn.com or calling us at 888-364-7621

Verifying Requests. To help protect the privacy of Canadian residents requesting to exercise their privacy rights (“Requestors”) and maintain security, we will take steps to verify the Requestors’ identity before granting access to their personal information or complying with their request. If a Requestor asks us to provide them with specific pieces of personal information, we may require the Requestor provide appropriate proof of identity.

Responding to Requests

For residents of Quebec:

Upon receiving a request to access, delete, or correct an error or omission, we will respond within thirty (30) days of its receipt.

For residents of Canadian Provinces other than Quebec:

Upon receiving a request to access, delete, or to correct an error or omission, we will respond within thirty (30) days of its receipt. If we require more time (up to an additional 30 days for a total of 60 days), we will inform the Requestor of the reason and extension period in writing.

For all residents of Canada:

We may deny the request if we cannot verify the individual’s identity or are legally permitted to deny the request, such as if processing it proves impossible or would involve disproportionate effort.

If we deny the request, we will explain the basis for the denial, provide or delete any personal information that is not subject to the denial, and refrain from using the personal information retained for any purpose other than permitted by the denial. We will maintain a record of the request and our response for 24 months. We do not charge a fee to process or respond to verifiable requests unless they are excessive, repetitive, or manifestly unfounded. If we determine that the request warrants a fee, we will tell the Requestor why we made that decision and provide them with a reasonable cost estimate before completing the request.

Other provisions pertaining to requests for personal information of minors or requests made by authorized agents shall apply as outlined in the Privacy Policy, above.

Sharing of Personal Information

We may disclose the categories of personal information identified in Personal Information We Collect, above, to the categories of entities listed below for our business or commercial purposes as further described in Purposes for Using, Disclosing, and Otherwise Processing Personal Information, in the Privacy Policy. Except as described in the Privacy Policy and this Addendum, we will not share personal information with a third party unless a customer requests the disclosure, consents to such disclosure, or the disclosure is required or allowed by law.

We may share your personal information with the below categories of individuals who may be located outside of Canada. If you are a resident of Quebec, we may transfer your personal information with the below categories of individuals who may be located outside of Quebec:

- Subsidiaries or affiliates located throughout Canada and in the US.
- Service providers who act for or on behalf of the Company in connection with the business of the Company, such as our IT operating system and platform vendors, security vendors, monitoring and data analytics providers, and payment service providers located throughout Canada and outside of Canada in the US.
- Other third parties, located throughout Canada and in the US, such as potential buyers in the event of a proposed or actual purchase, sale, lease, merger, amalgamation or any other type of acquisition, disposal, or financing of all or any portion of the Company or of any of the business assets or shares of the Company or a division thereof; to regulatory authorities or other third parties to comply with a law, regulation, search warrant, subpoena, judicial proceeding, a court order, or as otherwise may be required by law; to enforce our policies or contracts; to collect amounts owed to us; during emergencies when safety is at risk, as determined by the Company; otherwise where necessary for the establishment, exercise or defense of legal claims; and to other similar third parties where disclosure is required for an ordinary business purpose in connection with our provision of products or services.

Data Storage, Cross-Border Transfers, and Protection

The Company may store your personal information on servers and systems under its control or on servers and system that it licenses. To carry out the purposes described in our Privacy Policy and this Addendum your personal information may be transferred and stored outside of Canada, including in the United States. If you are a resident of Quebec, please note that your personal information may be transferred and stored outside of Quebec, including in other provinces in Canada and the United States, for these purposes. This means your data may be subject to the laws of other jurisdictions, which may not provide the same level of protection as in your province or in Canada generally. U.S. government or law enforcement agencies may access your data under U.S. law.

When the Company transfers personal data across borders to a third party, it will take all reasonable steps to protect the data from unauthorized use and disclosure. The Company will only engage third-party processors that have adequate security measures, policies, and staff training in place to safeguard personal information. The Company will proceed with a Privacy Impact Assessment as defined in the Quebec Privacy Act when required to ensure the safety of

your personal information. The Company may audit and inspect the third party's data handling and storage practices when necessary to ensure compliance with these protective measures.

Changes to this Canadian Privacy Addendum

The Company will update this Canadian Privacy Addendum occasionally. When the Company posts changes to this Canadian Privacy Addendum, we will also revise the "Addendum Last Updated" date below. The Company encourages you to review this Canadian Privacy Addendum periodically to be informed of how the Company is protecting your information and to be aware of any changes. Your continued use of the site after the posting of any amended Canadian Privacy Addendum shall constitute your agreement to be bound by any such changes. Any changes to this Canadian Privacy Addendum are effective immediately after being posted by the Company.

Addendum Last Updated: 12/31/2024