

## Dorsey & Whitney LLP HR Privacy Notice for U.S. Personnel

Dorsey & Whitney LLP, on behalf of itself, its subsidiaries and affiliates (collectively, “Dorsey”) provides this Dorsey & Whitney LLP HR Privacy Notice (“HR Privacy Notice”) to provide information to its partners, employees, temporary employees, job applicants, and contractors (collectively “Personnel”) – and other individuals whose Personal Data is collected for human resources purposes (such as qualified dependents) – regarding how we collect and use your Personal Data in connection with your partnership, employment or other relationship with Dorsey. In this Notice, “Personal Data” means data relating to identified or identifiable individuals and households.

This HR Privacy Notice applies only to Personal Data used in the context of human resources and employment or partnership purposes and other internal business functions relating to our Personnel and their family members or beneficiaries, including internal computer systems, networks, and online services. Dorsey’s [Data Privacy Policy Statement](#) describes how we collect, use and protect the Personal Data of individuals who use the Dorsey website ([www.Dorsey.com](http://www.Dorsey.com)) and other online services. The Privacy Policy will apply to the extent Dorsey Personnel use any services subject to the Privacy Policy.

Current Dorsey employees and partners can review and update much of their Personal Data via [UltiPro Self Service](#). If you have questions about other Personal Data, or if you are not a current employee or partner, you can contact [HRSupport@dorsey.com](mailto:HRSupport@dorsey.com) with questions about your Personal Data, or if you need to update your Personal Data.

### **GENERAL PURPOSES FOR COLLECTING, USING AND DISCLOSING PERSONAL DATA**

---

Dorsey collects Personal Data about its prospective, current and former Personnel and other individuals as appropriate in the context of an employment, partnership or contractual work relationship (such as dependents), including for recruitment and technology support services, and as needed for using internal software, networks and devices. The categories of Personal Data we process, along with representative data elements, are listed in the chart below. We may not collect from you or use all of the Personal Data identified below depending on your position or the nature of your relationship with Dorsey, but we have endeavored to provide a comprehensive list of all Personal Data we collect and use.

We generally use, disclose and retain Personal Data processed under this HR Privacy Notice for the following purposes:

- (a) Personal Data pertaining to **prospective** Personnel may be collected, used and shared for:
- Recruitment and staffing, including evaluation of skills and job placement.
  - Hiring decisions, including negotiation or determination of compensation, benefits, relocation packages, etc.
  - Risk management, including reference and other background checks.

- EEO/Affirmative Action programs.
- Our Business Purposes (defined below).

(b) Personal Data pertaining to **current** Personnel may be collected, used and shared for:

- Staffing and job placement, including scheduling and absence management.
- Verification of eligibility to work and compliance with immigration laws, rules and regulations.
- Administration of compensation, insurance and benefits programs.
- Time and attendance tracking, expense reimbursement, other workplace administration and facilitating relationships within Dorsey.
- Technology support uses, such as managing our computers and other assets, providing email and other tools to our workers.
- EEO/Affirmative Action and Diversity & Inclusion programs.
- Internal and external directories of Personnel.
- Health and wellness programs.
- Reasonable accommodations.
- Occupational health and safety programs (including required injury and illness reporting, disaster recovery and business continuity planning, and workers' compensation management).
- Health and safety requirements imposed by Dorsey, government authorities, or others, depending on work location, engagement or travel (e.g. vaccination status or health screening).
- Talent and performance development, skills management and training, performance reviews, performance management, employee feedback surveys, and recognition and reward programs.
- HR support services, such as responding to inquiries and providing information and assistance.
- Employee relations, such as implementing and administering Human Resources policies, investigations, and resolving issues or concerns that you may raise.
- Training, including technology support training and programs offered through Dorsey U.
- Risk management and loss prevention, including employee and premises monitoring.
- Implementing an effective sickness absence management system including monitoring the amount of leave and subsequent actions to be taken, such as making adjustments.
- Managing leave programs such as family and parental leave.
- Succession planning and adjustments for restructuring.
- Dorsey.com, including website biographies for attorneys and other professionals.
- As requested by individuals, including to verify employment or partnership and income (e.g. for mortgage applications).
- Nominations for external awards and recognition.
- Business Purposes.

(c) Personal Data pertaining to **former** Personnel may be collected, used and shared for:

- Re-employment.
- Administration of compensation, insurance and benefits programs.
- Expense reimbursements.
- For archival and recordkeeping purposes.
- Responding to claims for unemployment benefits and other government inquiries.
- As requested by individuals, including employment or partnership verifications.
- EEO/Affirmative Action programs.
- Business Purposes.

(d) Personal Data pertaining to individuals whose information is provided to Dorsey in the course of HR management (such as information pertaining to employees' family members, beneficiaries, dependents, emergency contacts, *etc.*) may be collected, used and shared for:

- Administration of compensation, insurance and benefit programs.
- Workplace administration.
- To comply with child support orders or garnishments.
- To maintain emergency contact lists and similar records.
- Business Purposes.

**Business Purposes** means the following purposes for which Personal Data may be collected, used and shared:

- Maintaining comprehensive and up-to-date Personnel records.
- Establishing, managing or terminating the employment, partnership or other working relationship.
- Maintaining a safe and respectful workplace and improving Personnel satisfaction and performance.
- Billing and collections, legal project management and pricing, staffing on client matters.
- Responding to RFPs or other client requests for information about Dorsey services and Personnel.
- Identity and credential management, including identity verification and authentication, issuing ID card and badges, system administration and management of access credentials.
- Security, loss prevention, information security and cybersecurity.
- Legal and regulatory compliance, including without limitation all uses and disclosures of Personal Data that are required by court orders and applicable laws, regulations, orders and ordinances, and for compliance with legally-mandated policies and procedures, such as anti-money laundering programs, security and incident response programs, intellectual property protection programs, and other processing in connection with the establishment and defense of legal claims.
- Corporate audit, analysis and consolidated reporting.

- To enforce our contracts and to protect Dorsey, our Personnel, our clients and their personnel and the public against injury, theft, legal liability, fraud or abuse, to people or property.
- As needed to de-identify the data or create aggregated datasets, such as for consolidating reporting, research or analytics.
- Making back-up copies for business continuity and disaster recovery purposes, and other IT support, debugging, security, and operations.
- For the analysis and improvement of technical and organizational services, operations, and similar matters.
- As needed to facilitate firm governance.

## CATEGORIES OF PERSONAL DATA

This chart describes the categories of Personal Data that Dorsey may collect in connection with its partnership, employment and contractual work relationships. Note: all Personal Data may be used and disclosed in connection with our Business Purposes.

Category of Personal Data & Representative Data Elements	Common Purposes for Collecting & Sharing
<p><b>Contact Data</b></p> <ul style="list-style-type: none"> <li>• Honorifics and titles, preferred form of address</li> <li>• Mailing address</li> <li>• Email address</li> <li>• Telephone number</li> <li>• Mobile number</li> </ul>	<p>We use your Contact Data to communicate with you by mail, email, telephone or text about your work relationship, including sending you compensation and benefits communications and other firm information.</p> <p>Contact Data is also used to help us identify you and personalize our communications, such as by using your preferred name.</p>
<p><b>Identity Data</b></p> <ul style="list-style-type: none"> <li>• Full name, nicknames or previous names (such as maiden names)</li> <li>• Date of birth</li> <li>• Language</li> <li>• Timekeeper/employee ID number</li> <li>• Dorsey account identifiers and passwords</li> <li>• Benefits program identifiers</li> <li>• System identifiers (e.g., usernames or online credentials)</li> </ul>	<p>We use your Identity Data to identify you in our HR records and systems, to communicate with you (often using your Contact Data) and to facilitate our relationship with you, for internal record-keeping and reporting, including for data matching and analytics, and to track your use of firm programs and assets, and for most processing purposes described in this HR Privacy Notice, including governmental reporting, employment or partnership verification, verification of right to work in the US, background checks, etc.</p>
<p><b>Government ID Data</b></p>	<p>We use your Government ID Data to identify you and to maintain the integrity of our HR records, enable</p>

<b>Category of Personal Data &amp; Representative Data Elements</b>	<b>Common Purposes for Collecting &amp; Sharing</b>
<ul style="list-style-type: none"> <li>• Social security/national insurance number</li> <li>• Driver’s license information</li> <li>• Passport information</li> <li>• Other government-issued identifiers as may be needed for risk management or compliance (<i>e.g., if you are a licensed attorney or other professional, we will collect your license number</i>)</li> </ul>	<p>employment or partnership verification and background screening, such as reference checks, license verifications, and criminal records checks (subject to applicable law), enable us to administer payroll and benefits programs and comply with applicable laws (such as reporting compensation to government agencies as required by law), as well as for security and risk management, such as collecting driver’s license data for employees who operate firm automobiles, professional license verification, fraud prevention and similar purposes.</p> <p>We may also use Government ID data for other firm and customer business purposes, such as collecting passport data and secure flight information for Personnel who travel as part of their job duties.</p>
<p><b>Biographical Data</b></p> <ul style="list-style-type: none"> <li>• Resume or CV</li> <li>• Application and screening questionnaires</li> <li>• Data from LinkedIn profiles and similar platforms and other information publicly available on the Internet</li> <li>• Social media or communications platform usernames or handles</li> <li>• Education and degree information</li> <li>• Employment, partnership or other work history</li> <li>• Professional licenses, bar or court admissions, certifications and memberships and affiliations</li> <li>• Personal and professional skills and talents summaries (<i>e.g., languages spoken, CPR certification status, community service participation</i>), interests and hobbies</li> <li>• Professional goals and interests</li> <li>• Criminal records</li> </ul>	<p>We use Biographical Data to help us understand our Personnel and for professional and personal development, to assess suitability for job roles, and to ensure a good fit between each individual’s background and relevant job functions.</p> <p>We also use Biographical Data to foster a creative, diverse workforce, for recruiting, for coaching, and to guide our decisions about internal programs and service offerings.</p>

Category of Personal Data & Representative Data Elements	Common Purposes for Collecting & Sharing
<p><b>Transaction and Interaction Data</b></p> <ul style="list-style-type: none"> <li>• Dates of employment or partnership</li> <li>• Re-employment eligibility</li> <li>• Position, Title, Reporting Information</li> <li>• Work history information</li> <li>• Compensation history (partners only as permitted by applicable laws)</li> <li>• Time and attendance records</li> <li>• Leave and absence records</li> <li>• Compensation/Payroll records</li> <li>• Benefit plan records</li> <li>• Timekeepers' time entries</li> <li>• Travel and expense records</li> <li>• Training records</li> <li>• Performance records and reviews</li> <li>• Exit interviews</li> <li>• Records of investigations</li> <li>• Disciplinary and performance management records</li> <li>• Offer letters and agreements</li> <li>• Partnership agreements</li> </ul>	<p>We use Transaction and Interaction Data as needed to manage the personnel relationship and fulfill standard human resources functions, such as scheduling work, providing payroll and benefits and managing the workplace (e.g. onboarding, maintenance, evaluations, performance management, investigations, etc.).</p>
<p><b>Financial Data</b></p> <ul style="list-style-type: none"> <li>• Bank account number and details</li> <li>• Firm-issued payment card information, including transaction records</li> <li>• Credit history, if a credit check is obtained (only for partners and in other limited circumstances)</li> <li>• Dorsey compensation history</li> <li>• Tax-related information</li> </ul>	<p>We use your Financial Data to facilitate compensation, (such as for direct deposits), expense reimbursement, to process financial transactions, for tax withholding purposes, and for security and fraud prevention.</p>
<p><b>Health Data</b></p>	<p>We use your Health Data as needed to provide health and wellness programs, including health insurance programs, and for internal risk management and</p>

<b>Category of Personal Data &amp; Representative Data Elements</b>	<b>Common Purposes for Collecting &amp; Sharing</b>
<ul style="list-style-type: none"> <li>• Medical information for accommodation of disabilities</li> <li>• Medical information for leave and absence management, emergency preparedness programs</li> <li>• COVID-19 testing and vaccination data, exposure to COVID-19, temperature, symptoms, travel, quarantines, and isolation status</li> <li>• Wellness program participation</li> <li>• Information pertaining to enrollment and utilization of health and disability insurance programs</li> <li>• Dietary restrictions</li> </ul>	<p>analytics related to our human resources functions, staffing needs, and other Business Purposes.</p> <p>In response to the COVID-19 pandemic, we have implemented health and other screening procedures, vaccination tracking, and other measures to reduce the possibility of transmission on our premises to our Personnel and guests and to comply with applicable public health orders and guidance. We use and may need to share this data to carry out contact tracing, implement and enforce workplace safety rules and for public safety reasons and compliance obligations.</p>
<p><b>Device/Network Data</b></p> <ul style="list-style-type: none"> <li>• Device information from devices that connect to our networks</li> <li>• System logs, including access logs and records of access attempts</li> <li>• Records from access control devices, such as badge readers</li> <li>• Information regarding use of IT systems and Internet access, including internet search and browsing history, metadata and other technically-generated data</li> <li>• Records from technology monitoring programs, including suspicious activity alerts</li> <li>• Data relating to the use of communications systems and the content of those communications</li> </ul>	<p>We use Device/Network Data for system operation and administration, technology and asset management, information security incident detection, assessment, and mitigation and other cybersecurity purposes. We may also use this information to evaluate compliance with firm policies. For example, we may use access logs to verify work hours and attendance records. Our service providers may use this information to operate systems and services on our behalf, and in connection with service analysis, improvement, or other similar purposes related to our business and HR functions.</p>
<p><b>Audio/Visual Data</b></p> <ul style="list-style-type: none"> <li>• Photographs</li> <li>• Video images, videoconference records</li> <li>• CCTV recordings</li> </ul>	<p>We use photographs on the firm’s internal and external website directories and in marketing materials and communications, including via social media. We may record Dorsey U and other firm-provided trainings for archival purposes and on-demand viewing.</p>

Category of Personal Data & Representative Data Elements	Common Purposes for Collecting & Sharing
<ul style="list-style-type: none"> <li>• Voicemails</li> </ul>	<p>We may use CCTV recording for premises security purposes and loss prevention. We may also use this information to evaluate compliance with firm policies. For example, we may use CCTV images to verify attendance records.</p>
<p><b>Inference Data</b></p> <ul style="list-style-type: none"> <li>• Performance reviews</li> <li>• Results of tests related to interests and aptitudes</li> </ul>	<p>We use inferred and derived data to help tailor professional development programs and to determine compensation and suitability for advancement or other positions. We may also analyze and aggregate data for workforce planning. Certain inference data may be collected in connection with information security functions, e.g. patterns of usage and cybersecurity risk.</p>
<p><b>Compliance and Demographic data</b></p> <ul style="list-style-type: none"> <li>• Employment or work eligibility verification records, background screening records, and other records maintained to demonstrate compliance with applicable laws, such as payroll tax laws, immigration laws, ADA, FMLA, ERISA <i>et al.</i></li> <li>• Occupational safety records and worker’s compensation program records</li> <li>• Records relating to internal investigations</li> <li>• Records of privacy and security incidents involving HR records, including any security breach notifications</li> </ul>	<p>We use Compliance and Demographic Data for internal governance, firm ethics programs, institutional risk management, reporting, demonstrating compliance and accountability externally, and as needed for litigation and defense of claims.</p>
<p><b>Protected Category Data</b></p> <p>Characteristics of protected classifications under state or federal law, e.g. race, national origin, religion, gender, disability, marital status, sexual orientation, or gender identity.</p>	<p>We use Protected Category Data as needed to facilitate the employment, partnership or other relationship, to respond to surveys and client requests for information, for compliance and legal reporting obligations (including Affirmative Action), to evaluate the diversity of our Personnel and the success of our diversity and inclusion efforts, and as needed for litigation and defense of claims.</p>



## CATEGORIES OF SOURCES OF PERSONAL DATA

We collect Personal Data from various sources, which vary depending on the context in which we process that Personal Data.

- **Data you provide us** – We will receive your Personal Data when you provide them to us, when you apply for a position, complete forms, via UltiPro Self Service, complete your timesheets, provide information via a Dorsey app (e.g. the COVID-19 self check-in process) or otherwise direct information to us.
- **Data from a third party** – We will receive your Personal Data from third parties such as recruiters, credit reporting agencies or employment / partnership screening providers.
- **Data from publicly available sources** – We may collect data that is publicly available on the Internet (e.g. through a Google search of a candidate’s name).
- **Data we collect automatically** – We may also collect information about or generated by any device you have used to access internal IT services, applications and networks.
- **Data we receive from Service Providers** – We receive information from service providers performing services on our behalf.
- **Data we create or infer** – We (or third parties operating on our behalf) create and infer Personal Data such as Inference Data based on our observations or analysis of other Personal Data processed under this Privacy Notice, and we may correlate this data with other data we process about you. We may combine Personal Data about you that we receive from you and from third parties.

## DISCLOSURE OF PERSONAL DATA

---

We generally process HR Personal Data internally; however, it may be shared or processed externally by third party service providers, when required by law or necessary to complete a transaction, or in other circumstances described below.

## CATEGORIES OF INTERNAL RECIPIENTS

The Personal Data identified below collected from our Personnel may be disclosed to the following categories of recipients in relevant contexts.

- **Personnel of HR, Diversity & Inclusion, Marketing, Professional Development and Lawyer Recruiting Departments** – All Personal Data relating to these functions.
- **Personnel of Finance Departments** – Personal Data to the extent related to payroll, compensation, expense reimbursements, billing, collections, pricing or legal project management, Dorsey store purchases, etc.
- **Supervisors and Managers** – Elements of Personal Data to the extent necessary to evaluate, establish, and maintain the partnership, employment or contractual relationship, evaluate staffing levels, conduct reviews, handle compliance obligations, and similar matters.

- **Department managers searching for new employees or contractors** – Personal data of job candidates contained in job applications to the extent allowed by relevant laws and departmental needs.
- **IT Administrators** of Dorsey and/or third parties who support the management and administration of HR processes may receive Personal Data as necessary for providing relevant IT related support services (conducting IT security measures and IT support services).
- **Peers and colleagues** – Elements of Personal Data in connection with firm directories, firm and interpersonal communications, and other contexts relevant to the day-to-day operation of firm business.

### CATEGORIES OF EXTERNAL RECIPIENTS

Dorsey may provide HR Personal Data to external third parties as described below. The specific information disclosed may vary depending on context, but will be limited to the extent reasonably appropriate given the purpose of processing and the reasonable requirements of the third party and Dorsey. We generally provide information to:

- Our subsidiaries and affiliates.
- Service providers, vendors, and similar data processors that process Personal Data on Dorsey's behalf (e.g., analytics companies, financial analysis/budgeting, trainings, benefits administration, payroll administration, travel agencies, employment or partnership and income verifications, background checks, etc.) or that provide other services for our Personnel or for Dorsey.
- To prospective seller or buyer of such business or assets in the event Dorsey sells or buys any business or assets.
- To future Dorsey affiliated entities, if Dorsey or substantially all of its assets are acquired by a third party, in which case Personal Data held by it about its employees and contractors will be one of the transferred assets.
- To your employment or professional references, in order to inform them that you have applied with Dorsey as part of our recruiting process.
- To future prospective employers seeking to confirm your relationship with Dorsey.
- To government agencies or departments or similar parties in connection with employment or partnership related matters, attorney licensure or bar admission.
- To clients and potential clients, including in pitches or responses to RFPs and as part of Dorsey's billing and collection processes.
- To any public authority in relation to national security or law enforcement requests, if Dorsey is required to disclose Personal Data in response to lawful requests by a public authority.
- To any other appropriate third party, if Dorsey is under a duty to disclose or share your Personal Data in order to comply with any legal obligation or to protect the rights, property, health, or safety of Dorsey, our Personnel, customers or others.

## **LOCATIONS OF RECIPIENTS**

Dorsey and some Dorsey affiliates are located in the United States. Any Personal Data collected under this Policy will likely be processed in the United States, in addition to any other jurisdiction where such Dorsey affiliate is located.

## **DATA ADMINISTRATION**

---

### **SECURITY**

Dorsey requires that Personal Data be protected using technical, administrative, and physical safeguards, as described in our [Information Security Policy](#). Dorsey staff must follow the security procedures set out in applicable security policies at all times.

### **RETENTION AND DISPOSAL**

Dorsey keeps Personal Data only for the amount of time it is needed to fulfill the legitimate business purpose for which it was collected or to satisfy a legal requirement. Dorsey staff must follow any applicable records retention schedules and policies and destroy any media containing Personal Data in accordance with applicable policies.