

# Instinet Incorporated – Employee, Job Applicant, and Contractor Privacy Policy

22 June 2023



## **CONTENTS**

1.0.	How We Use Personal Information .....	3
1.1.	How We Use Sensitive Personal Information.....	4
2.0.	Collection and Disclosure of Personal Information: .....	5
3.0.	Sources and Disclosures of Personal Information .....	7
4.0.	Additional Information for California Residents.....	9
4.1.	Retention Period .....	10
4.2.	Individual Rights and Requests .....	10
4.3.	Authorized Agents .....	11
4.4.	De-Identified Information .....	11
5.0.	Cookies and Third Party Analytics .....	11
6.0.	Marketing emails .....	11
7.0.	Jurisdiction and Cross-Border Transfer .....	11
8.0.	Third-Party Services.....	12
9.0.	Children's Privacy.....	12
10.0.	Changes to This Policy .....	12
11.0.	Questions or Comments .....	12

Instinet Incorporated and its subsidiaries located in the United States (collectively “**Instinet**,” “**we**,” or “**us**”) value the information entrusted to us. The purpose of this Employee, Job Applicant and Contractor Privacy Policy (the “**Policy**”) is to notify you and your family members of the processing of Personal Information that we collect, use, and disclose in the context of your current or former role as our job applicants, employees, and individuals providing professional services to us.

The Policy also applies to the individuals who are on your health plan and the beneficiaries of your retirement accounts, as well as your emergency contacts. It is your responsibility to inform any such individuals about this Policy and ensure that you have the right to provide their Personal Information to us.

## **1.0. HOW WE USE PERSONAL INFORMATION**

“Personal Information” is information that identifies, relates to, or could reasonably be linked with a particular individual. This section describes how we may use the Personal Information detailed in the “Collection and Disclosure of Personal Information” section below. The details of our collection and disclosure of Personal Information are found in the next sections.

We use your Personal Information, in accordance with applicable laws, to:

- Receive and process job applications;
- Manage the candidate selection process;
- Evaluate your suitability for the position(s) you are applying for;
- Communicate with you about your respective applications, respond to your inquiries, and notify you of applicable terms and policies;
- Conduct reference checks;
- Conduct background checks;
- Analyze and monitor the diversity of job applicants;
- Make an offer of employment;
- Contact you about future career opportunities;
- Process payroll, manage wages and other awards such as stock options, stock grants and bonuses, reimburse expenses and provide healthcare, pensions, savings plans and other benefits;
- Fulfill administrative functions, such as aggregated management reporting, statistical analyses, internal training, and as generally required to conduct our business;
- Plan and manage workforce activities and personnel generally, including for recruitment, onboarding, appropriate staffing, performance management, training and career development, payments and benefit administration, and promotions;
- Conduct workforce assessments, including determining physical or mental fitness for work and evaluating work performance;
- Operate, maintain, monitor and secure our facilities, equipment, systems, networks, applications and infrastructure;
- Allow you to access and utilize office equipment, cafeteria, vending machines, and other systems/services that can be accessed via your access badge;
- Manage attendance, time keeping, leaves of absence and vacation;
- Facilitate personnel communication and workforce travel;

- Facilitate personnel relocation and/or immigration;
- Sign up or invite you to in person or virtual events;
- Undertake quality and safety assurance measures, protect the health and safety of our workforce and others, and conduct risk and security control and monitoring;
- Conduct research, analytics, and data analysis, such as to assist in succession planning and to ensure business continuity, as well as to design personnel retention programs and diversity initiatives, in accordance with applicable law;
- Perform identity verification, accounting, budgeting, audit, and other internal functions, such as internal investigations, disciplinary matters and handling grievances and terminations;
- Operate and manage IT and communications systems and facilities, allocate Instinet assets and human resources, and undertake strategic planning and project management; and
- Comply with law, legal process, requests from governmental or regulatory authorities, internal policies and other requirements such as, conflict of interest prevention, securities laws/regulations/obligations compliance, broker-dealer laws/regulations/obligations compliance, financial institution laws/regulations/obligations compliance, income tax deductions, record-keeping, equal employment opportunity laws, work permit and immigration regulations and reporting obligations, and the exercise or defense of legal claims.

We use your family members' Personal Information to:

- Facilitate payments and benefit administration for benefits applicable to your family members;
- Facilitate relocation and/or immigration of your family members;
- Contact, in an emergency, your family members that you designate as your emergency contacts;
- Comply with law, legal process, requests from governmental or regulatory authorities, internal policies and other requirements such as, conflict of interest prevention, securities laws/regulations/obligations compliance, broker-dealer laws/regulations/obligations compliance, financial institution laws/regulations/obligations compliance, income tax deductions, record-keeping, work permit and immigration regulations and reporting obligations, and the exercise or defense of legal claims that may require your family members' Personal Information; and
- Sign up or invite your family members to in person or virtual events.

### **1.1. How We Use Sensitive Personal Information**

In connection with you and your family members' Sensitive Personal Information (please see the last row in the Personal Information About You/Your Family Members tables in the next section for definition), we use such information for purposes of performing services for our business, providing services as requested by you, and ensuring the security and integrity of our business, providing infrastructure, and the individuals we interact with, establishing and maintaining your working relationship with us, countering malicious, deceptive, fraudulent, or illegal actions, ensuring the diversity of our workforce, complying with legal obligations, managing payroll and corporate credit card or account use, administering and providing benefits, and securing the access to, and use of, our facilities, equipment, systems, networks, applications, and infrastructure, and other collection and processing that is not for

the purposes of inferring characteristics about an individual. We do not use Sensitive Personal Information beyond these purposes.

## 2.0. COLLECTION AND DISCLOSURE OF PERSONAL INFORMATION:

These charts explain how your and your family’s Personal Information may be collected, processed, and disclosed to third parties, both at the date of this policy and for the prior twelve months.

<b>PERSONAL INFORMATION ABOUT YOU</b>		
<b>Categories of Personal Information About You</b>	<b>Sources of Personal Information</b>	<b>Recipients of Disclosures of Personal Information</b>
<b>Identifiers and Personal Information (as defined in the California customer records law)</b> , such as name, address, contact information, unique personal identifiers, IP address that can reasonably be linked or associated with a particular resident or household, email address, account name, online identifiers, photo badges, beneficiary designations and government-issued identifiers (e.g., Social Security number, driver’s license number, passport number), signature, financial information, education and employment information, physical characteristics or description.	See rows 1-9, 11, and 12 in the <i>Sources of Personal Information</i> table below	See rows 1-11 in the <i>Recipients of Disclosures of Personal Information</i> table below
<b>Protected Class Information</b> , such as characteristics of protected classifications under California or federal law, such as sex, age, gender, race, disability, medical conditions, citizenship, military/veteran status, gender identity and expression, primary language, political affiliation/activities, immigration status, marital status, and requests for leave.	See rows 1-9, and 11 in the <i>Sources of Personal Information</i> table below	See rows 1, 3, 6, and 7 in the <i>Recipients of Disclosures of Personal Information</i> table below
<b>Commercial Information</b> , such as transaction information and purchase history, including information about corporate credit card purchases, frequent flyer rewards, expenses submitted for reimbursement, and other travel-related programs and expenses	See rows 1, 4, and 6 in the <i>Sources of Personal Information</i> table below	See rows 1, 3, 6, 7, and 10 in the <i>Recipients of Disclosures of Personal Information</i> table below
<b>Personal Investments and Outside Business Activity Information</b> , such as your brokerage accounts, and you outside business affiliations	See rows 1, 3, and 6 -8 in the <i>Sources of Personal Information</i> table below	See rows 1, 3, and 7 in the <i>Recipients of Disclosures of Personal Information</i> table below
<b>Biometric Information</b> , such as fingerprints	See row 1 in <i>Sources of Personal Information</i> table below	See row 11 in the <i>Recipients of Disclosures of Personal Information</i> table below

<b>PERSONAL INFORMATION ABOUT YOU</b>		
<b>Categories of Personal Information About You</b>	<b>Sources of Personal Information</b>	<b>Recipients of Disclosures of Personal Information</b>
<b>Internet or network activity information</b> , such as access and usage information regarding websites, applications and systems, information about online communications, including browsing and search history, timestamp information, and access and activity logs	See rows 1 and 8 in the <i>Sources of Personal Information</i> table below	See rows 1, 5 and 8 in the <i>Recipients of Disclosures of Personal Information</i> table below
<b>Geolocation Data</b> , such as device location, and approximate location derived from IP address	See rows 1 and 8 in the <i>Sources of Personal Information</i> table below	See row 8 in the <i>Recipients of Disclosures of Personal Information</i> table below
<b>Audio/Video Data</b> . Audio, electronic, visual and similar information, such as photographs and call and video recordings, including voicemail and security camera footage, information about the use of electronic devices and systems, key card usage, and photos on websites or in employee directories	See rows 1, 2, 4, 10, and 11 in the <i>Sources of Personal Information</i> table below	See rows 1, 2, 3, 7, and 9 in the <i>Recipients of Disclosures of Personal Information</i> table below
<b>Education Information</b> subject to the federal Family Educational Rights and Privacy Act such as student transcripts, grade point average, grades, academic standing and disciplinary records, confirmation of graduation	See rows 1-7, 11, and 12 in the <i>Sources of Personal Information</i> table below	See rows 1, 2, 4, and 10 in the <i>Recipients of Disclosures of Personal Information</i> table below
<b>Employment Information</b> . Professional or employment-related information, such as work history and prior employer, information from reference checks, work experience, qualifications, training and skills, work authorization, CV, résumé, cover letter, professional and other work-related licenses, permits and certifications held, and publicly accessible information posted on your professional social media accounts, background screening information, employment application, membership in professional organizations, personnel files, personal qualifications and training, eligibility for promotions and other career-related information, work preferences, business expenses, wage and payroll information, benefit information, information on leaves of absence or PTO, performance reviews, information on internal investigations or disciplinary actions	See rows 1-8 in the <i>Sources of Personal Information</i> table below	See rows 1-3, and 7 in the <i>Recipients of Disclosures of Personal Information</i> table below
<b>Personal Profile Information</b> . Information you may provide in connection with a personality evaluation such as a Myers-Briggs assessment	See rows 1, 4 in the <i>Sources of Personal Information</i> table below	See row 1 in the <i>Recipients of Disclosures of Personal Information</i> table below

<b>PERSONAL INFORMATION ABOUT YOU</b>		
<b>Categories of Personal Information About You</b>	<b>Sources of Personal Information</b>	<b>Recipients of Disclosures of Personal Information</b>
<b>Inferences</b> drawn from any of the Personal Information listed above to create a profile about, for example, an individual's preferences, characteristics, predispositions, and abilities	From any of the categories of information listed in this table and corresponding sources	See row 1 in the <i>Recipients of Disclosures of Personal Information</i> table below
<p><b>Sensitive Personal Information.</b></p> <ul style="list-style-type: none"> <li>Personal Information that reveals an individual's Social Security, driver's license, state identification card, or passport number; account log-in; racial or ethnic origin, religious or philosophical beliefs, citizenship, immigration status, or union membership; the contents of mail, email, and text messages unless Instinet is the intended recipient of the communication;</li> <li>Personal Information collected and analyzed concerning an individual's sex life or sexual orientation.</li> </ul>	See rows 1-9, and 11 in the <i>Sources of Personal Information</i> table below	See rows 1, 3, and 5-7 in the <i>Recipients of Disclosures of Personal Information</i> table below

### 3.0. SOURCES AND DISCLOSURES OF PERSONAL INFORMATION

This section describes our sources of Personal Information and parties to who such Personal Information may be disclosed. These tables should be reviewed together with the information in the "Collection and Disclosure of Personal Information" section above.

<b>Sources of Personal Information</b>
1. From you directly (or from someone you authorize) when you seek employment with us, request information from us, register for our events as an applicant or employee, visit our websites as an applicant or employee, or complete forms as part of your onboarding and employment
2. From our affiliates when you (or someone you authorize to act on your behalf) seek employment with us or request information from us through our affiliates
3. From our business partners when you (or someone you authorize to act on your behalf) seek employment with us or request information from us through our business partners
4. From third party service providers involved in your recruitment, training, evaluation, payroll, travel planning, expense reimbursement, relocation, benefits, or other human resource functions to whom you provide your information
5. From you in your communications with us (e.g., your email address, your signature block, and/or other information you include in your communications)
6. From third-party service providers engaged for Know Your Customer (KYC) services, Anti-Money Laundering (AML) services, and/or transaction monitoring and screening services in our efforts to comply with laws and regulations and to prevent/investigate of bad acts related to your application for employment or employment with us
7. From government and regulator watch lists and the media as part of our efforts to comply with

laws and regulations and to prevent/investigate of bad acts related to your application for employment or employment with us
8. From our or our service providers' technological tools such as service logs, cookies, activity trackers, IT security software and systems, or pixel tags that obtain such information from your personal or corporate devices in connection with your employment or your interactions with our systems
9. From third party providers of security services for our offices, such as security desk or video monitoring,
10. From third party providers of business communications monitoring services
11. From third party providers of event, entertainment, training, or conference services who may capture you on photo, video, or audio and may obtain your identification or credentials in connection with the services they provide
12. From the references you provide us

<b>Recipients of Disclosures of Personal Information</b>
<p>1. Our affiliates – for example:</p> <ul style="list-style-type: none"> <li>in connection with your recruitment or role at Instinet when your role could involve working with our affiliates</li> <li>in connection with functions shared among Instinet and its affiliates such as IT, human resources, training, and events</li> <li>in connection with catalogues shared among Instinet and its affiliates such as personnel directories, personnel contact information, personnel biographies, organization charts, and the like</li> </ul>
<p>2. Our business partners - for example:</p> <ul style="list-style-type: none"> <li>in connection with your role in performing services for or with the business partners of Instinet</li> </ul>
<p>3. Third party service providers of Know Your Customer (KYC) and Anti-Money Laundering (AML) services, transaction monitoring and screening services, communications monitoring services – for example:</p> <ul style="list-style-type: none"> <li>in connection with your role as an applicant, employee, or contractor at Instinet and our efforts to comply with laws and regulations and to prevent/investigate of bad acts related to your application for employment or employment with us</li> </ul>
<p>4. Third party service providers of event, entertainment, training, or conference services - for example:</p> <ul style="list-style-type: none"> <li>when such vendors need the information in order to assist Instinet in putting on the event, entertainment, or training involving you</li> </ul>
<p>5. Third party service providers of technology services potentially used by you as part of your role or potential role at Instinet such as video conferencing, electronic communications, fintech services - for example:</p> <ul style="list-style-type: none"> <li>when the information is needed for permissioning you as a user of third party software and systems utilized in your role with Instinet such as trading platforms, productivity software, communications and video conferencing utilities, telephonic systems</li> </ul>



6. Third party service providers of relocation, immigration, travel, payroll, healthcare, office support and other human resource services and benefits, for example:

- when we utilize third-party software or technology services in providing you our various human resources functions such as payroll and expense submissions
- when we sign you up for training
- when we sign you up with benefit providers
- when we sign you up for immigration or relocation assistance services
- when we sign you up for office support systems and services like copy machine access, locker access, vending machine and cafeteria payment systems

7. Public, governmental, and regulatory authorities – for example:

- when such disclosures are obligatory for your role with Instinet

8. Third party providers of security and IT security services - for example:

- when your information is needed by office/building security personnel or for access badge control systems in our offices.
- when your information is needed to monitor, protect, locate, activate, deactivate, recover, format or otherwise secure the corporate devices assigned to you as part of your role with Instinet

9. Third party providers of telephone/other-communication regulatory recording services – for example:

- when you, or an organization you represent, seek our services that must be conducted on a recorded telephone line or via recorded communications

10. Third party consultants – for example

- When we engage consultants to advise us regarding aspects of our business that you are involved in

11. Third party providers of fingerprinting services – for example

- when your fingerprints need to be submitted to a regulator

#### 4.0. ADDITIONAL INFORMATION FOR CALIFORNIA RESIDENTS

Pursuant to the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act (collectively, the “CCPA”), we are providing the following additional details regarding the Personal Information that we collect, use, and disclose about California residents.

**We do not “sell” or “share” your Personal Information, including your Sensitive Personal Information, as defined under the CCPA. We have not engaged in such activities in the 12 months preceding the date this Policy was last updated.**

Without limiting the foregoing, we do not “sell” or “share” the Personal Information, including the Sensitive Personal Information, of minors under 16 years of age.

#### 4.1. Retention Period

We retain Personal Information for as long as needed or permitted in light of the purpose(s) for which it was collected. The criteria used to determine our retention periods include:

- The duration of your employment or contract with us;
- The length of time we have an ongoing relationship with you or your dependents/beneficiaries and the length of time thereafter during which we may have a legitimate need to reference your Personal Information to address issues that may arise;
- Whether there is a legal obligation to which we are subject (for example, certain laws may require us to keep your employment or personnel records for a certain period of time); and
- Whether retention is advisable in light of our legal position (such as in regard to applicable statutes of limitations, litigation or regulatory investigations).

#### 4.2. Individual Rights and Requests

If you are a California resident and you believe we have collected your Personal Information, you may make the following requests:

1. You may request that we disclose to you the following information:
  - a. The categories of Personal Information we collected about you and the categories of sources from which we collected such Personal Information;
  - b. The business or commercial purpose for collecting Personal Information about you; and
  - c. The categories of Personal Information about you that we otherwise disclosed, and the categories of third parties to whom we disclosed such Personal Information (if applicable).
2. You may request to correct inaccuracies in your Personal Information.
3. You may request to have your Personal Information deleted.
4. You may request to receive the specific pieces of your Personal Information, including a copy of the Personal Information you provided to us in a portable format.

You have the right to be free from unlawful discrimination for exercising your rights under the CCPA.

To make a request, please contact us at [Americasprivacy@nomura.com](mailto:Americasprivacy@nomura.com) or (833) 770-4090. We will verify and respond to your request consistent with applicable law, taking into account the type and sensitivity of the Personal Information subject to the request. We may need to request additional Personal Information from you, such as mailing address, telephone number and/or email address, in order to verify your identity and protect against fraudulent requests. If you maintain a password-protected account with us, we may verify your identity through our existing authentication practices for your account and require you to re-authenticate yourself before disclosing or deleting your Personal Information. If you make a deletion request, we may ask you to verify your request before we delete your Personal Information.

California law also gives residents of California the right, under certain circumstances, to request information from us regarding the manner in which we share certain categories of Personal Information with third parties for their direct marketing purposes. To request such information, please contact using the contact information provided in the "Questions and Comments" section, above.

#### **4.3. Authorized Agents**

If an agent would like to make a request on your behalf as permitted by applicable law, the agent may use the submission methods noted in the section entitled “Individual Rights and Requests.” As part of our verification process, we may request that the agent provide, as applicable, proof concerning their status as an authorized agent. In addition, we may require that you verify your identity as described in the section entitled “Individual Requests” or confirm that you provided the agent permission to submit the request.

#### **4.4. De-Identified Information**

Where we maintain or use de-identified information, we will continue to maintain and use the de-identified information only in a de-identified fashion and will not attempt to re-identify the information.

### **5.0. COOKIES AND THIRD PARTY ANALYTICS**

Cookies are pieces of information stored directly on your computer. Cookies allow us to collect such information as browser type, time spent on the Services, pages visited, language preferences, and traffic data. We use the information for security purposes, to facilitate navigation, to display information more effectively, and to personalize your experience. We also gather statistical information about use of the Services in order to continually improve their design and functionality, understand how they are used, and assist us with resolving questions regarding them. We do not currently respond to browser do-not-track signals. If you do not want information collected through the use of cookies, most browsers allow you to automatically decline cookies or be given the choice of declining or accepting particular cookies from a particular website. You may also wish to refer to <http://www.allaboutcookies.org/manage-cookies/index.html>. If, however, you do not accept cookies, you may experience some inconvenience in your use of the Services.

We may work with certain third parties to collect Personal Information and to engage in analytics, auditing, research, and reporting. These third parties may use tracking mechanisms such as web logs and pixel tags, and they may set and access cookies on your computer or device. In particular our site uses Google Analytics to collect and analyze certain information about the website’s visitors. This service may also collect information regarding the use of other websites, apps, and online services. Information regarding Google’s practices with Google Analytics can be found in Google’s privacy policy at <http://www.google.com/policies/privacy/partners> and choices for “opt-out” opting out are described at <https://tools.google.com/dlpage/gaoptout>.

### **6.0. MARKETING EMAILS**

If you no longer want to receive marketing emails from us on a going-forward basis, you may opt-out by clicking the “unsubscribe” link at the bottom of each such email. If you opt out, we may still send you important administrative messages, from which you cannot opt out.”

### **7.0. JURISDICTION AND CROSS-BORDER TRANSFER**

We are located in the United States. We may store and process your Personal Information in any country where we have facilities or in which we engage service providers. By using our Services, you understand that your information will be transferred to countries outside of your country of residence, including the United States, which may have data protection rules that are different from those of your country.

## **8.0. THIRD-PARTY SERVICES**

This Policy does not address, and we are not responsible for, the privacy, information, or other practices of any third parties, including any third party operating a website or service to which the Services link. The inclusion of a link on the Services does not imply our endorsement of the linked site or service.

## **9.0. CHILDREN'S PRIVACY**

Our Corporate Group Websites and other services are not directed to individuals under the age of 13, and we do not knowingly collect Personal Information from individuals under 13. As used in this Privacy Policy ("Policy"), the term "Corporate Group Websites" refer to [www.instinet.com](http://www.instinet.com).

## **10.0. CHANGES TO THIS POLICY**

The "Last Updated" legend at the top of this Policy indicates when this Policy was last revised. Any changes will become effective when we post the revised Policy at <https://www.instinet.com/privacy-policy>.

## **11.0. QUESTIONS OR COMMENTS**

If you have any questions or comments regarding our privacy practices or this Policy, please contact us by email at [Americasprivacy@nomura.com](mailto:Americasprivacy@nomura.com) or by mail at: c/o Legal and Compliance Department, Instinet, LLC, 309 West 49th Street, New York, NY 10019.