ICONIQ Capital Global Employee and Employment Candidate Privacy Notice

ICONIQ Capital and Affiliates
Effective Date: February 2026

1. PURPOSE AND SCOPE

This Global Employee and Employment Candidate Privacy Notice ("Global Privacy Notice") describes how ICONIQ Capital LLC, ICONIQ Capital (Singapore) Pte Ltd, ICONIQ Capital (UK) Ltd, and their affiliates (collectively, "ICONIQ," "we," "our," or "us") collect, use, disclose, and otherwise process the personal information of employees and candidates for employment across our global operations.

This Global Privacy Notice applies to all current employees, prospective employees, contractors, and prospective contractors of ICONIQ and its affiliates (collectively, "you" or "your") and is designed to meet the requirements of applicable privacy and data protection laws in the United States (including California), the United Kingdom, and Singapore.

IMPORTANT: This Global Privacy Notice is limited to ICONIQ's practices related to the collection, processing, and sharing of personal information in connection with employment and recruitment activities. This notice is not intended to cover ICONIQ's practices related to the collection, processing, or sharing of information for other purposes related to its business, including but not limited to client data, investor data, portfolio company data, or other business-related information. Clients, investors, prospective clients, prospective investors, and other persons seeking information regarding ICONIQ's privacy practices related to ICONIQ's services should refer to the relevant Privacy Notice of ICONIQ Capital available at https://www.iconiqcapital.com/privacy/privacy-policies.

2. JURISDICTIONS COVERED

This Global Privacy Notice is intended for use specifically in the following jurisdictions:

- Singapore
- United States (Excluding California)
- United States (California)
- United Kingdom (and European Economic Area, where applicable)

3. APPLICATION TO CANDIDATES IN OTHER JURISDICTIONS

If you are an employee or candidate for employment with ICONIQ Capital who is currently located in a jurisdiction other than the United States, the United Kingdom, or Singapore, you acknowledge and agree that by submitting your personal information to ICONIQ Capital for the purposes of employment or potential employment, you are applying for or maintaining a position within the United States, the United Kingdom, and/or Singapore as relevant to your role, and that your personal information will be collected, processed, and treated in accordance with this Global Privacy Notice and the applicable

jurisdiction-specific provisions set forth below depending on the location of your employment or prospective employment.

By submitting your application or accepting employment with ICONIQ Capital, you acknowledge and agree that your personal information will be transferred to and processed in the United States, the United Kingdom, and/or Singapore, and will be subject to the privacy and data protection laws applicable in those jurisdictions.

4. JURISDICTION-SPECIFIC PROVISIONS: SINGAPORE

Personal Data Information for Employees and Job Candidates in Singapore

Where our processing of your personal information is governed by the Personal Data Protection Act 2012 of Singapore ("PDPA"), this Section applies in relation to you.

Collection, Use and Disclosure of Personal Data

We collect, use, and disclose personal data of employees and job candidates in accordance with the PDPA and relevant employment laws. Such personal data may be collected directly from you, or through authorised third parties such as recruitment agencies, background check providers, or referees.

The personal data we collect may include, but is not limited to:

- Identification details (e.g., name, NRIC or passport number, nationality, date of birth);
- Contact details (e.g., address, telephone number, email address);
- Employment history, qualifications, and references;
- Financial / bank account information for payroll and benefits administration;
- Medical and health-related information (for employment suitability, insurance, or workplace safety);
- Background check and verification data; and
- Any other information reasonably required for employment, performance, or compliance purposes.

Purpose of Collection and Use

We collect, use, and disclose personal data of employees and job candidates only for reasonable and lawful purposes, including:

- Assessing and evaluating suitability for employment or engagement;
- Managing recruitment, onboarding, and employment relationships;
- Administering payroll, benefits, tax, and insurance matters;
- Managing performance, promotion, disciplinary, and termination processes;
- Complying with applicable laws, regulations, and internal policies (e.g., CPF, tax, immigration, and manpower requirements);
- Ensuring workplace health, safety, and security; and
- Responding to legitimate business, legal, or regulatory obligations.

Where applicable, we will obtain your consent for the collection, use, or disclosure of personal data unless an exception under the PDPA applies (for example, legitimate interests with appropriate assessment and safeguards, evaluative purposes, investigations or proceedings, vital interests/emergencies, or where required or authorised by law).

Retention and Protection of Personal Data

We retain personal data for as long as necessary to fulfil the purposes outlined above, or as required under applicable laws. When no longer required, personal data will be securely destroyed, anonymised, or deleted in accordance with our data retention policy.

We implement reasonable administrative, physical, and technical safeguards to protect personal data against unauthorised access, collection, use, disclosure, or similar risks.

Accuracy

We will take reasonable steps to ensure personal data is accurate and complete if it is likely to be used to make a decision affecting an individual or to be disclosed to another organisation.

Overseas Transfers

We may transfer personal data outside Singapore (including to ICONIQ group entities and service providers). We will ensure the recipient provides a standard of protection comparable to the PDPA (for example, through legally enforceable obligations), or rely on an applicable PDPA exception where permitted.

Data Breach Management

We maintain processes to assess, contain, and remediate data incidents. Where a breach is notifiable, we will notify the PDPC as soon as practicable and no later than 3 calendar days after determining notifiability, and notify affected individuals as soon as practicable where required (including where the breach is likely to result in significant harm or involves ≥500 individuals).

Access, Correction, and Withdrawal of Consent

Employees and candidates in Singapore may request access to, or correction of, their personal data, or withdraw consent for its continued use or disclosure by contacting our Data Protection Officer (DPO) using the business contact information below.

Business Contact Information (Singapore):

- Post: ICONIQ Capital (Singapore) Pte. Ltd., 18 Robinson Road, #24-01/02, 18 Robinson, Singapore 048547
- Email: legalnotices@iconiqcapital.com (routes to the DPO team)
- Tel: +65 6817 6164 (Mon-Fri, 9am-6pm SGT)

We may need to verify your identity. We will generally respond within 30 calendar days. Certain PDPA exceptions may apply. Where we correct personal data, we will (where practicable) send the corrected data to other organisations to which the data was disclosed within the past year, or annotate the record if a correction is not made.

Upon withdrawal of consent, we will cease the collection, use, or disclosure of personal data unless such processing is required or authorised under the PDPA or other written law, or an applicable consent exception applies. Withdrawal of consent may affect our ability to proceed with employment, recruitment, or related HR functions; where relevant, we will inform you of such consequences. We may continue to retain personal data to the extent necessary for legal or business purposes.

Complaints and Contact

Questions or complaints regarding our handling of personal data may be directed to the Data Protection Officer using the contact details listed above. If a matter is not resolved satisfactorily, you may refer it to the PDPC:

Website: www.pdpc.gov.sg Tel: +65 6377 3131 Email: info@pdpc.gov.sg

5. JURISDICTION-SPECIFIC PROVISIONS: UNITED STATES EXCLUDING CALIFORNIA

Privacy Notice for Employees and Job Candidates in the United States (Excluding California)

This Section applies to employees and candidates for employment with ICONIQ Capital, LLC and its affiliates who are located in the United States but outside of California. If you are located in California, please refer to Section 6 of this Global Privacy Notice for information specific to California residents.

Collection of Personal Information

We collect personal information from employees and job candidates in connection with employment and recruitment activities. Such personal information may be collected directly from you or through authorized third parties such as recruitment agencies, background check providers, former employers, or references.

The categories of personal information we may collect include, but are not limited to:

- Identifiers (e.g., name, Social Security number, driver's license number, passport number, date of birth);
- Contact information (e.g., address, telephone number, email address);
- Employment history, qualifications, education, and professional references;
- Financial and bank account information for payroll and benefits administration;
- Tax-related information;
- Background check and verification data;
- Medical and health-related information (for employment suitability, benefits administration, or workplace safety, where permitted by law);
- Emergency contact and beneficiary information; and
- Any other information reasonably required for employment, performance management, or compliance purposes.

Purposes for Collection and Use

We collect, use, and disclose personal information of employees and job candidates for legitimate business purposes, including:

- Assessing and evaluating suitability for employment or engagement;
- Managing recruitment, onboarding, and employment relationships;
- Administering payroll, benefits, tax withholding, and insurance matters;

- Managing performance, promotion, disciplinary, and termination processes;
- Complying with applicable federal, state, and local laws, regulations, and internal policies (including tax, immigration, and employment laws);
- Ensuring workplace health, safety, and security;
- Conducting background checks and verifications as permitted by law;
- Responding to legitimate business, legal, or regulatory obligations; and
- Facilitating internal business operations and administration.

Disclosure of Personal Information

We may disclose your personal information to the following categories of recipients:

- ICONIQ group entities and affiliates for internal administrative purposes;
- Service providers who perform services on our behalf, including payroll processors, benefits administrators, background check providers, IT service providers, and professional advisors;
- Government agencies and regulatory authorities as required by law;
- Third parties in connection with legal proceedings, investigations, or as otherwise required or permitted by law; and
- Third parties in connection with a merger, acquisition, or sale of assets, where your personal information may be transferred as part of such transaction.

We do not sell your personal information to third parties.

Retention of Personal Information

We retain personal information for as long as necessary to fulfil the purposes outlined above, or as required under applicable federal, state, or local laws. When no longer required, personal information will be securely destroyed, anonymized, or deleted in accordance with our data retention policies and applicable legal requirements.

Data Security

We implement reasonable administrative, physical, and technical safeguards designed to protect personal information against unauthorized access, collection, use, disclosure, or similar risks.

Employee Rights

Under applicable federal law, employees and candidates may have certain rights with respect to their personal information, including the right to access personnel records in accordance with applicable state laws and company policies. Employees may also have rights under specific federal statutes, including the right to request access to certain records maintained by the employer. To the extent additional rights are provided under applicable state or federal law, we will comply with such requirements.

Contact Information

If you have any questions or concerns regarding this Privacy Notice or our handling of your personal information, please contact us at:

- Post: ICONIQ Capital, LLC, 50 Beale St, Ste. 2300, San Francisco, CA 94105
- Email: legalnotices@iconiqcapital.com

- Tel: (415) 967-7763

6. JURISDICTION-SPECIFIC PROVISIONS: CALIFORNIA

PRIVACY NOTICE FOR CALIFORNIA CONSUMERS

The California Consumer Privacy Act (with any implementing regulations and as may be amended from time to time "CCPA") imposes certain obligations on ICONIQ Capital, LLC (collectively, "ICONIQ", "we", "our" or "us") as a "business" and grants certain rights to California Residents ("California Resident," "you" or "your") with regard to "personal information" (as defined under the CCPA). This Privacy Notice for California Consumers ("California Privacy Notice") contains disclosures required by the CCPA, including our **Notice at Collection**, information surrounding how and why we collect, use, and disclose personal information and your potential rights with regard to your personal information under the CCPA. This California Privacy Notice is only relevant to residents of California, and applies only to the collection or other use of "personal information" that is subject to the CCPA. Terms used herein have the meaning ascribed to them in the CCPA. The rights described herein are subject to exemptions and other limitations under applicable law.

Notice at Collection and Use of Personal Information

Information We Collect

Depending on how you interact with us we may collect the following categories of personal information from or about you, including:

Category	Examples
Identifiers	A real name, alias, email address, postal address, Internet Protocol (IP) address, account name, Social Security number, driver's license number, passport number, or other similar personal identifiers.
Other personal information categories, as listed in the California Customer Records statute (Cal. Civ. Code § 1798.80(e))	A signature, physical characteristics or description, telephone number, insurance policy number, education, certification & designation, current employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information.
Protected classification characteristics under California or federal law	Age (40 years or older), race/ethnicity, citizenship, marital status, gender, veteran, disability, or military status.
Commercial information	Account activity, records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.

Professional or employment-related information	Current or past job history or performance evaluations.
Education-related information	Transcripts, grade point averages, diplomas, certificates of achievement, and disciplinary records.
Audio, visual, or similar information	Pictures or recorded events.
Internet or other electronic network activity information	Interactions with our website or use of certain online tools, Internet usage, and IP addresses.
Inferences drawn from other personal information	Profile reflecting a person's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.
Sensitive personal information	Passport number, driver's license, state identification card, social security number, racial or ethnic origin, philosophical beliefs, or union membership.

Purpose for Collecting and Using Personal Information

Depending on how you interact with us, we may use and collect the personal information we collect for one or more of the following business or commercial purposes, including:

- Processing job applications and assessing candidate suitability and qualifications for specific positions;
- Conducting background checks and verification of employment history, qualifications, and credentials;
- Managing the recruitment and hiring process, including interview scheduling and candidate communications;
- Conducting reference checks with previous employers and professional contacts;
- Onboarding new employees and establishing employee records;
- Administering employee benefits, compensation, and payroll;
- Managing employee performance reviews and career development;
- Ensuring workplace safety and compliance with employment laws and regulations;
- Investigating workplace complaints or concerns;
- Managing employee training and professional development programs;

- Workforce planning and talent management;
- Processing work authorization and visa requirements for employment eligibility;
- Administering employee departure processes, including exit interviews and offboarding;
- Maintaining alumni or former candidate databases for future opportunities; and
- Other commercial purposes related to employment.

How Long We Keep Information

How long we keep your personal information will vary primarily depending on the purpose for which we are using your personal information and our legal obligations. The retention period will be determined by various criteria, including the purposes for which we are using it (as it will need to be kept for as long as is necessary for any of those purposes) and our legal obligations (as laws or regulations may set a minimum period for which we have to keep your personal information). In general, we will retain your personal information for as long as is necessary to provide the relevant services and where laws or regulations set a minimum period for which we are required to keep certain of your personal information.

Sale or Sharing of Personal Information

We do not sell or share your personal information (as such terms are defined under the CCPA).

Our Collection, Use, and Disclosure of Personal Information and Sensitive Personal Information

Information We Have Collected

In the preceding 12 months, and depending on how you interact with us, we may have collected the categories of personal information listed above in "Information We Collect."

Sources of Personal Information

We may collect personal information from certain categories of sources, including:

- Directly from you as part a job application or creating an employment profile;
- Professional networking platforms (e.g., LinkedIn);
- Recruitment agencies and executive search firms;
- Educational institutions and professional certification bodies;
- Professional references provided by candidates;
- Background check and screening service providers;
- Previous employers (for reference checks and employment verification);
- Job boards and recruitment websites;
- Career fairs and networking events;
- Immigration and visa processing service providers;

- Employee referral programs;
- Publicly available professional profiles and publications;
- Testing and assessment service providers;
- Your communications with us and our service providers;
- Your and our service providers, including but not limited to: administrators, custodians, brokers, auditors, law firms, accountants, consultants, employment agencies, credit bureaus, other financial institutions;
- Our affiliates or our affiliates' service providers; and
- Government entities and other publicly available directories and sources.

Purposes for Collecting and Using Personal Information

We may collect your personal information for the business or commercial purposes described above in "Purpose for Collecting and Using Personal Information."

Our Disclosure of Personal Information

We do not sell or share your personal information (as those terms are defined under the CCPA). We do not knowingly sell or share the personal information of California Residents under 16 years old. In the preceding 12 months, we may have disclosed for a business purpose the following categories of personal information to the following categories of third parties, as described in the following chart:

Category of Personal Information	Category of Third Party
Identifiers (for example your name, address, SSN, IP address, account name, driver's license number, passport number, or other similar personal identifiers)	• Payroll and benefits administration service providers • Employee benefits providers (insurance companies, pension administrators, health plan providers) • Immigration lawyers and visa processing service providers • Occupational health providers and medical assessment services • Employee training and development providers • Employee assistance program providers • Workers' compensation insurers • Recruitment marketing and employer branding service providers • Video interviewing and assessment platform providers • Employee onboarding technology providers • Human resources information system (HRIS) providers • Time and attendance tracking system providers • Performance management platform providers • Learning management system providers • Drug testing and health screening service providers
Other personal information categories, as listed in the California Customer Records statute (Cal. Civ. Code § 1798.80(e)) (for example, a signature, financial	

information, or bank account information)	• Government agencies and regulatory bodies (for employment eligibility verification, tax withholding, and compliance reporting) • Former employers and professional references (when conducting reference checks) • Entities used for job application or candidate screening and tracking. • Business partners, including consultants and advisors. • Technical service providers. • Professional services organizations, such as auditors and law firms. • Affiliated entities.
Professional or employment-related information (for example, job history or performance evaluations)	
Education-related information (for example, transcripts, grade point averages, diplomas, certificates of achievement, and disciplinary records)	
Commercial information (for example, account activity, records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies)	
Inferences drawn from other personal information (for example, a profile reflecting a person's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes)	

Protected classification characteristics under California or federal law (for example, race/ethnicity, citizenship, marital status, gender, veteran, disability, or military status)	• Payroll and benefits administration service providers • Employee benefits providers (insurance companies, pension administrators, health plan providers) • Immigration lawyers and visa processing service providers • Occupational health providers and medical assessment services • Employee assistance program providers • Workers' compensation insurers • Human resources information system (HRIS) providers • Government agencies and regulatory bodies (for employment eligibility verification, tax withholding, and compliance reporting) • Professional services organizations, such as auditors and law firms. • Affiliated entities.

In addition, we may disclose and in the preceding 12 months may have disclosed all of the categories of personal information identified above in the section, "Information We Collect," to the following categories of third parties: (i) judicial courts, regulators, or other government agents purporting to have jurisdiction over us, our subsidiaries or our affiliates, or opposing counsel and parties to litigation; and (ii) other third parties as may otherwise be permitted by law. We may also transfer to another entity or its affiliates or service providers some or all information about you in connection with, or during negotiations of, any merger, acquisition, sale of assets or any line of business, change in ownership control, or financing transaction. We may disclose personal information to all of the third parties listed above to comply with our legal obligations or for the business or commercial purposes identified above in "Purposes for Collecting and Using Personal Information."

We may disclose your personal information to our service providers such as our fund administrator, CRM provider, IT providers, or email providers, other entities that have agreed to limitations on the use of your personal information, or entities that fit within other exemptions or exceptions in or as otherwise permitted by the CCPA. We also may disclose personal information about you or your accounts to a third party at your request or direction or with your consent.

Use and Disclosure of Sensitive Personal Information

As noted above in "Personal Information We Collect", under the CCPA, certain personal information we collect and process may be considered "sensitive personal information." The CCPA requires that we provide you with a right to limit our use or disclosure of such sensitive personal information in certain circumstances. Currently, we are not using your sensitive personal information for purposes that would require that we provide you with a right to limit.

Rights of California Consumers

The CCPA provides California consumers the following rights, subject to certain exceptions and limitations:

- *Be Informed*. To be informed, at or before the point of collection, of the categories of personal information to be collected and the purposes for which the categories of personal information shall be used;

- *Request to Know*. The right to request (a) the categories and specific pieces of personal information we collect, use, disclose, and sell about you, (b) the categories of sources from which we collected

your personal information, (c) our purposes for collecting or selling your personal information, (d) the categories of your personal information (if any) that we have either sold or disclosed for a business purpose, and (e) the categories of third parties with which we disclosed or sold personal information;

- *Request to Delete*. Request that we delete the personal information we have collected from you or maintain about you (subject to certain exceptions);
- *Request to Correct*. Request that we correct inaccurate personal information;
- *Opt-Out of Sale*. Request that we do not "sell" (as that term is defined in the CCPA) your personal information; (we do not);
- *Opt-Out of Sharing*. Request to opt-out of the "sharing" (as that term is defined in the CCPA) of your personal information if a business shares your personal information with third parties (we do not);
- *Limit Use and Disclosure of Sensitive Personal Information*. Request to limit the use and disclosure of sensitive personal information where required by the CCPA (please note that we are not using your sensitive personal information for purposes that would require that we provide you with such right to request to limit); and
- *Not to Be Discriminated Against*. Not to receive discriminatory treatment for the exercise of the privacy rights conferred by the CCPA.

The CCPA does not restrict our ability to do certain things like comply with other laws or comply with regulatory investigations. In addition, the CCPA does not apply to certain information like personal information collected, processed, sold or disclosed pursuant to the federal Gramm-Leach-Bliley Act and its implementing regulations. We also reserve the right to retain, and not to delete, certain personal information after receipt of a Request to Delete from you where permitted by the CCPA or another law or regulation.

Shine the Light

For certain categories of personal information, you may have the right to request a list of what personal information (if any) we disclosed to third parties for their own direct marketing purposes in the past 12 months and the names and addresses of those third parties.

How to Submit a Request

You may submit Request to Know, Request to Correct or a Request to Delete ("Consumer Rights Request"), as described above or other applicable California law to us via phone (855) 636-4357 or email CCPAinquiries@iconiqcapital.com.

Verifying Requests

We are only required to respond to verifiable Consumer Rights Requests made by you or your legally authorized agent. When you submit a Consumer Rights Request, we may ask that you provide clarifying or identifying information to verify your request, which may include, depending on the sensitivity of the information you are requesting and the type of request you are making, your name and email address. Any information gathered as part of the verification process will be used for verification purposes only.

Authorized Agents

You are permitted to designate an authorized agent to submit a Consumer Rights Request on your behalf and have that authorized agent submit the request through the aforementioned methods. In order to be able to act, authorized agents have to submit proof that they are authorized to act on your behalf, or have a power of attorney. We may also require that you directly verify your own identity with us and directly confirm with us that you provided the authorized agent permission to submit the request.

Changes to this Privacy Policy

We may update this California Privacy Notice from time to time and to reflect changes in our personal information practices. We encourage you to review the most current California Privacy Notice provided to you.

Contact for More Information

If you have any questions or concerns about this California Privacy Notice, or to request this US and California Privacy Notice in an alternative format, please contact us at Phone: (415) 967-7763, Post: ICONIQ Capital, 50 Beale St, Ste. 2300, San Francisco, CA 94105, or Email: legalnotices@iconiqcapital.com.

This California Privacy Notice for employees and employment candidates was last updated February 2026. Copies of our other privacy policies can be found at https://www.iconiqcapital.com/privacy/privacy-policies.

7. JURISDICTION-SPECIFIC PROVISIONS: UNITED KINGDOM (AND EUROPEAN ECONOMIC AREA)

About this Notice

This Staff Privacy Notice applies to staff and prospective staff of ICONIQ Capital (UK) Ltd (and any wholly owned subsidiaries) based in the United Kingdom (UK) and European Economic Area (EU) (if applicable) (the "Firm", "we" or "us").

For the purposes of UK and EU data protection laws, the relevant "controller" of your personal data is, usually, the entity that employs or engages you (or may potentially employ or engage you, if you are a prospective employee or contractor). In the UK, the controller will be ICONIQ Capital (UK) Ltd. It is the "controller" of your personal data that decides how and why your personal information is held and used.

The Firm are required under UK and EU data protection legislation to notify you of the information contained in this Privacy Notice.

The Firm values the privacy of those who provide personal information to us. Please read this Privacy Notice carefully to understand how the Firm handles your personal information. This Privacy Notice describes what personal information we collect about our employees and potential employees, contractors and potential contractors based in the UK and EU, how we use and otherwise process it, the basis upon which we process it, with whom it is shared, and how it is stored.

This notice also describes other important topics relating to information privacy.

1. Who does this notice apply to?

1.1 This Privacy Notice applies to all employees, prospective employees, contractors and prospective contractors of the Firm who are based in the UK and EU.

1.2 It applies to all of your personal data that we process in the context of your employment, prospective employment, engagement or prospective engagement in the UK / EU (as applicable).

2. Data protection principles

The Firm will comply with applicable data protection and privacy laws. These provide that the personal data we hold about you must be:

- used lawfully, fairly and in a transparent way;
- collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes;
- relevant to the purposes we have told you about and limited only to those purposes;
- accurate and kept up to date, kept only as long as necessary for the purposes we have told you about; and
- kept securely.

3. The information that we hold about you

3.1 Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data which cannot be linked to an individual in any way (i.e. anonymous data).

3.2 There are "special categories" of more sensitive personal data which require a higher level of protection and we have set out more details about this at section 7 below.

3.3 Information collection

3.4 We collect, store and use any of the following categories of information about you and we refer to this as "personal information" or "personal data" throughout this Privacy Notice:

- your personal details: name and title, gender, birth date, national insurance number/social security number, home address and home/personal phone number and email address and proof of identification and address and marital status;
- your family's details: emergency contact information, spouse or civil partner name and contact information, spouse's or civil partner's national insurance number, names of dependents and co-insured family members' details;
- documentation required under immigration laws: citizenship details, national identification number, other documents required to show your right to live in your current country and to work for the Firm there and details required for residency, work permit and/or visa processes;
- employment/compensation records and information:

- current and any former titles and positions held with us (and information about such positions, including start date, how long in position, location of position/place of work, employee identification number, promotions, training records, overall work history, disciplinary actions, grievances, retirement eligibility, transfers);
- identification or verification search results, including employment searches, and references (subject to applicable law);
- current and historic compensation or terms with or provided/offered by us, base salary, bonus, pension contributions, commissions, benefits, sales compensation plans and information relating to any such plans or benefits;
- work contact information (phone number, postal address, mailing address, email address);
- your photo;
- performance reviews and information (including any career development plans), conduct and capability information and training records;
- work place accident information, sickness absence information and medical or health information (relevant to your employment and/or provided by you to us, for example, medical assessments and occupational health reports), records of any disabilities;
- work hours/pattern and annual leave information (including overtime and shift work, hours worked, breaks and department standard hours);
- absence information and details of any leave taken (for any reason);
- travel bookings, expense related claims, records and information;
- details regarding the termination of your employment or engagement, including the leaving date and reason for leaving and exit interviews; and
- written, electronic and phone communications.

- payroll data: bank details, working time records, current compensation, tax and social security information, IDs related to payroll processing and student loan information (where applicable);
- system and application access data: information required to access Firm systems and applications (such as system ID);
- talent management/resume/CV information: when you apply for a job or work with us/for us, we need to collect and hold details contained in an application and resume/CV or otherwise provided to or obtained by us, including personal and contact details, previous employment background, professional qualifications and memberships, references. We may also collect and hold career development and skills analysis, training, education, departmental changes, performance and calibration details;

- management records: details of any shares or options of common stock or directorships that you may hold; and
- miscellaneous information.

4. How is your information collected?

4.1 The Firm will receive most of this personal information from you directly (including through the application and recruitment process), although we may also receive some of this information from third parties, such as recruitment agencies, social media or online searches (including LinkedIn), training providers, medical professionals or occupational health providers, former employers or public agencies. The Firm will collect additional personal information in the course of job-related activities throughout the period of you working for us.

4.2 The Firm may collect this information in a variety of ways. For example, data might be collected through application forms, CVs/resumes, obtained from your passport or other identity documents such as your driving licence, from forms completed by you at the start of or during employment/engagement (such as benefit nomination forms), from correspondence with you, or through interviews, meetings or other assessments.

5. Use of personal information

5.1 The Firm will collect, use and store your personal information for a number of purposes, including those set out in 'Appendix 1 - Lawful Grounds for processing Personal Data' of this Privacy Notice.

5.2 Your family and emergency contact information: Separately, the Firm may process personal information about your family, next of kin, emergency contacts or nominated beneficiaries, for the provision of benefits or so that we can contact them in an emergency type situation. If you disclose information about your family to us or include it in written, electronic or phone communications, we may also have access to this in our systems. If you share personal information with us that relates to other people (for example, former employees or your next of kin), you will need to check with that person that they are happy for you to share it with us, and for us to use it in accordance with this Privacy Notice.

6. Legal bases for using your personal information

6.1 In order to comply with UK and EU data privacy laws, the Firm needs to have legal bases for using your personal information for the purposes set out in this Privacy Notice. We have set out some more detailed examples about the legal bases we rely on to process your data in 'Appendix 1 - Lawful Grounds for processing Personal Data'. The Firm considers that in nearly all cases, our legal basis will be one or more of the following:

- our use of your personal information is necessary for the performance of our obligations under our contract with you (for example, to pay you, communicate with you or to confer a benefit under the terms of your employment contract); or
- our use of your personal information is necessary for complying with our legal obligations, particularly as your employer/engager (or prospective employer/engager) (for example, providing

employee personal information to HMRC or an applicable regulator (e.g. the FCA), health and safety at work or conducting legally required checks on your right to work in the UK); or

- where our use of your personal information is not necessary for the performance of our contractual obligations, or compliance with our legal obligations, it is necessary for the purposes of our legitimate interests or the legitimate interests of a third party (for example, to enable us to centralise our HR systems and to use dedicated third party systems, to ensure a safe working environment, to ensure the reliability of our employees or to maintain adequate personnel records).

6.2 Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal information.

6.3 Where we are relying on our legitimate interests or the legitimate interests of a third party, we have explained, in this Privacy Notice, what those legitimate interests are.

7. Why we collect and use sensitive personal data

7.1 Sensitive personal data, so called "special categories" of personal data, require higher levels of protection. We need to have further justification for collecting, storing and using this. Special category data is personal data relating to racial or ethnic origins; political opinions; religious and philosophical beliefs; trade union membership; genetic data; biometric data; health data; sex life or sexual orientation. The Firm may process special categories of personal data in the following general circumstances:

- In limited circumstances, with your explicit written consent.
- Where we need to carry out our legal obligations and/or exercise rights conferred on us by law and in line with our data protection and information handling policy.
- Where it is needed in the public interest, such as, in some circumstances, for equal opportunities monitoring or in relation to an occupational pension scheme, and in line with our data protection and information handling policy.
- Where it is needed to assess your working capacity on health grounds, subject to appropriate confidentiality safeguards.
- Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is needed to protect your (or someone else's) interests and you are not capable of giving your consent, or where you have already made the information public.

7.2 The Firm will use sensitive personal data in the following ways:

- We will use information relating to leaves of absence, which may include sickness absence or family related leaves, to comply with employment and other laws and to administer benefits including statutory maternity pay, statutory sick pay, pensions and health insurance;
- We will use information about your physical or mental health, or disability status, to ensure your health and safety in the workplace and to assess your fitness to work, to provide appropriate workplace adjustments, to monitor and manage sickness absence and to administer benefits including statutory maternity pay, statutory sick pay, pensions and permanent health insurance; and

- If you leave employment and the reason for leaving is determined to be ill-health, injury or disability, we will use information about your physical or mental health, or disability status in reaching a decision about your entitlements under any applicable benefits or incentive plans.

7.3 The Firm does not need your consent if we use special categories of your personal data in accordance with this Privacy Notice to carry out our legal obligations or exercise specific rights in the field of employment law. In limited circumstances, we may ask you for your written consent to allow us to process certain particularly sensitive data. If we do so, we will provide you with details of the information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent. You should be aware that it is not a condition of your contract with the Firm that you agree to any request for consent from us for the processing of your personal information or special categories of personal data. Consent may be withdrawn at any time by contacting the Compliance department - see section 15 of this Privacy Notice for more information on this.

7,4 The Firm does not currently request or gather any information regarding political opinions, philosophical belief or trade union membership.

8. Information about criminal convictions

8.1 Where appropriate, the Firm may collect information about criminal convictions as part of the recruitment process or we may be notified of such information directly by you in the course of you working for us.

8.2 As part of the recruitment process (and senior manager promotion process), the Firm may engage a third party provider to carry out such background checks on our behalf relating to criminal convictions (in the UK, these are referred to as DBS checks); education history; credit rating; adverse media; prior employment history; global sanctions and enforcement; conduct; ID and, right to work. Such checks are repeated periodically for existing employees. In the absence of an FCA-regulatory obligation to carry out DBS checks, we and our third-party provider rely upon your explicit consent as the appropriate ground and condition for processing of such data.

8.3 We may use information about criminal convictions to make a decision about your recruitment, appointment or promotion. We are allowed to use your personal information in this way to carry out our legal and FCA-regulatory obligations (DBS checks are mandatory for senior managers), in the course of our legitimate business interests (including public interest, protecting our business and people, network and information security, preventing improper use of systems and protecting our workforce) and/or in reliance upon your explicit consent. We have in place an appropriate policy and safeguards which we are required by law to maintain when processing such data.

9. Monitoring

The Firm reserves the right to monitor, audit, copy, store or delete any network traffic over our systems. This includes a right to retrieve or access the contents of messages, inboxes or to undertake searches of our email systems for the purposes of monitoring or investigating wrongful acts, to comply with any of our legal or regulatory obligations, or, occasionally to ensure the effective operation of our business (for example in the event of unexpected absence and where access to business emails is required). Anything learned by us as a result of such monitoring may be used in relation to disciplinary proceedings. All monitoring activities will be undertaken in accordance with the laws that apply to us.

10. How we share your personal information (and who with)

10.1 The Firm may have to share your data with third parties, including third-party service providers and other entities in our group.

10.2 We require third parties to respect the security of your data and to treat it in accordance with the law. Please see section 11 for more information about the basis upon which we transfer your data outside the UK and EU (as applicable).

10.3 Disclosure within the Firm's group:

- Your business related information may be made available to other employees, temporary staff and contractors of the Firm and with customers, suppliers and agencies of the Firm in the course of administering your employment or providing our services. This includes your name, work contact details, position related information, employee photo and other related details.
- Your personal information may be shared with any entity that is a member of the Firm's group, where it is in our legitimate interests to do so for internal administrative purposes, to effectively operate the employment relationship with you and/or the workforce generally, for management purposes, corporate strategy, auditing and monitoring, system maintenance support and hosting of data and/or research and development. Access to your personal information is limited to those employees who need to know the personal information, and may include your managers and their designees, as well as employees in the HR, recruitment, corporate services, legal, information technology, and finance departments.
- The Firm may also share your personal information with group companies where they provide products and services to us, such as IT systems, data hosting, HR services, legal support, payroll and benefits administration and recruitment.

10.4 Disclosure to other third parties:

- The Firm will share your personal data with third parties where required by law, where it is necessary to administer the working relationship with you or where we have another legitimate interest in doing so.
- The Firm will share your personal information with the following categories of third parties:
    - other parties such as legal and regulatory authorities, accountants, auditors, lawyers and other outside professional advisors;
    - customers, clients or suppliers; and
    - companies that provide products and services to us, such as:
        - payroll providers and our bank;
        - benefits and pension providers/administrators;
        - insurance companies, including those providing medical insurance and group income protection (and our insurance brokers);
        - training providers and travel/hotel/venue providers;
        - parties requesting an employment reference for you;
        - HR services, such as external advisors, application tracking providers/systems;

- third party providers who carry out background checks;
- cloud storage providers;
- police and immigration authorities;
- occupational health assessment providers and medical professionals; and/or
- IT systems suppliers and support, including providers of HR systems and benefits management, email archiving, telecommunications suppliers, back-up and disaster recovery and cyber security services; and other outsourcing providers, such as contract lease management, and off-site storage providers.

- Where applicable, we will also disclose your personal information to third parties in some other circumstances:
  - if we sell or buy any business or assets, we may disclose your personal information to the prospective seller or buyer of such business or assets;
  - if the Firm or substantially all of its assets are acquired by a third party, in which case personal information held by the Company will be one of the transferred assets;
  - if we are under a duty to disclose or share your personal information in order to comply with any legal or regulatory obligation, any lawful request from government or law enforcement officials or applicable regulator and as may be required to meet national security or law enforcement requirements or prevent illegal activity;
  - to enforce our contract with you, to respond to any claims, to protect our rights or rights of a third party, to protect the safety of any person or to prevent any illegal activity; and/or
  - to protect the rights, property or safety of the Company, our employees or other persons.

10.5 Restrictions on use of your personal information by those we share it with.

10.6 Some of these companies may use your data in countries which are outside of the UK / EU (as applicable). We have included more details about this at section 11 below.

10.7 Any third parties with whom we share your personal information are limited (by law and/or by contract) in their ability to use your personal information and the purposes for which they use it. In respect of third party service providers who are processing data on our behalf, we only permit them to process personal data for specified purposes and in accordance with our instructions.

10.8 Other than as we have set out in this Privacy Notice, we will not share your personal information with any third party without notifying you and/or obtaining your consent. Where our actions are based on you having given your consent for us to use your information in a particular way, but you later change your mind, you should contact the Compliance department to notify us of this and we will stop doing so.

11. Transfers of information

11.1 We may transfer personal information relating to you outside of the UK and EU (as applicable) to staff working for us outside of the UK / EU, or other members of our group or third parties located outside of the UK / EU, for the purposes mentioned in section 5. Please be aware that countries which are outside the UK / EU may not offer the same level of protection for personal information as in the UK

/ EU, although our collection, storage and use of your personal information will continue to be governed by this Privacy Notice.

11.2 When transferring personal information outside the UK, we will:

- ensure that the country in which your personal information will be processed has been deemed "adequate" by the relevant UK authorities and/or by the European Commission (as applicable); or
- include the standard contractual data protection clauses approved by relevant authorities in the UK / EU (as applicable) for transferring personal information outside the UK / EU, into our contracts with other members of our group or third parties.

11.3 Further details on the steps we take to protect your personal information in these cases is available from us on request by contacting us at the Compliance department.

12. Retention of personal information

12.1 The Firm has identified retention guidelines for different types of HR data taking into account the purpose for which data is collected, statutory obligations in respect of the retention of data and limitation periods for the bringing of claims where the data may be evidentially relevant.

12.2 The indicative retention periods are:

- **recruitment records**: 6 months after the later of the point of collection, notification to candidates of the outcome of the recruitment exercise or last contact with the candidate on this. Recruitment information may be transferred to a successful candidate's employment file to the extent it is relevant to the ongoing relationship. The Firm retains personal information following recruitment exercises to demonstrate, if required, that candidates have not been discriminated against on prohibited grounds and that recruitment exercises are conducted in a fair and transparent way; and
- **personnel records**: while employment continues and up to 7 years after employment ceases. However, the Firm will review your records at intervals during employment and upon termination of employment to assess whether earlier deletion of any particular record is appropriate (where the data is no longer required for the purposes for which it was collected and any relevant limitation periods have expired).

12.3 In some circumstances we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you.

12.4 Once it is no longer necessary to retain your personal information, we will securely destroy it in accordance with applicable laws and regulations.

13. Change of purpose

13.1 The Firm will only use your personal data for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal data for an unrelated purpose, we will notify you and we will explain the lawful basis which allows us to do so.

13.2 Please note that we may process your personal data without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

14. Your rights

14.1 You have certain rights in relation to your personal information. If you would like further information in relation to these or would like to exercise any one of them, please contact the Compliance department. In certain circumstances, you have the right to request that we:

- provide you with a copy of any personal information which we hold about you;
- update any of your personal information which is out of date or incorrect or incomplete;
- delete any personal information which we hold about you if it is no longer necessary in relation to the purposes for which it was collected or processed (or, in some instances, where you have withdrawn your consent or objected to the processing);
- restrict the way that we process your personal information;
- provide your personal information to a third party;
- consider any valid objections which you have to our use of your personal information (where we are relying on our legitimate interests (or those of a third party) as the basis for the processing or that the processing is in the public interest); and
- provide a copy of any agreement under which your personal data is transferred outside of the UK / EU (as applicable).

14.2 The Firm will consider all such requests and provide our response within the time period stated by applicable law. Please note, however, that certain personal information may be exempt from such requests in certain circumstances, which may include if we need to keep processing your personal information for our legitimate interests or to comply with a legal obligation. There will be certain circumstances where the right does not apply to you under law and we will review this when we consider a request.

14.3 The Firm may request you provide us with information necessary to confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

14.4 You will not have to pay a fee to access your personal information (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

14.5 If you have any questions or concerns about our use of your personal information, please contact the Compliance department.

15. Right to withdraw consent

15.1 In the limited circumstances where the Firm's processing is based on your having provided consent to the collection, processing and transfer of your personal data for a specific purpose, you have the right to withdraw your consent for that specific processing at any time.

15.2 To withdraw your consent, please contact the Compliance department. Where these circumstances apply, once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

16. Keeping us updated

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your working relationship with us.

17. Security

17.1 The Firm is committed to protecting personal information from loss, misuse, disclosure, alteration, unauthorised access and destruction and takes all appropriate precautions to safeguard the confidentiality of personal information. Although we make every effort to protect the personal information which you provide to us, the transmission of information over the internet is not completely secure. As such, you acknowledge that we cannot guarantee the security of your personal information transmitted to us over the internet that any such transmission is at your own risk. Once we have received your personal information, we will use strict procedures and security features to prevent unauthorised access.

17.2 Where we have given you (or where you have chosen) a password which enables you to access any account with us, you are responsible for keeping this password confidential. We ask you not to share a password with anyone.

18. Automated decision-making

Automated decision-making takes place when an electronic system uses personal information to make a decision without human intervention, and that decision produces a legal or similarly significant effect on you (for example, this would be the case if we decided whether to offer you a job solely based on automated processing of your personal information). The Firm does not engage in that type of automated decision-making and we will notify you in writing if this position changes.

19. Third party websites

You may, from time to time, during your employment, access links to or other websites operated by third parties (e.g. training providers, industry news sources and bulletins). Please note that this Privacy Notice only applies to the personal information that we collect from or about you and we cannot be responsible for personal information collected and stored by third parties. Third party websites have their own terms and conditions and privacy policies, and you should read these carefully before you submit any personal information to these websites. The Firm does not endorse or otherwise accept any responsibility or liability for the content of such third party websites or third party terms and conditions or policies.

20. Changes to this Privacy Notice

This Privacy Notice does not form part of any employee's contract of employment or appointment or engagement agreement/terms and we may amend it from time to time. Any significant changes the Firm makes to this Privacy Notice in the future will be notified to you in writing. Please check back frequently to see any updates or changes.

21. Further questions or making a complaint

21.1 If you have any queries or complaints about our collection, use or storage of your personal information, or if you wish to exercise any of your rights in relation to your personal information, please

contact Technology Support and/or the Compliance department. We will investigate and attempt to resolve any such complaint or dispute regarding the use or disclosure of your personal information.

21.2 You may also make a complaint to the relevant data protection supervisory authority. In the UK, this is the Information Commissioner's Office (https://ico.org.uk/). Alternatively, you may seek a remedy through local courts if you believe your rights have been breached.

The practices described in this Privacy Notice statement are current personal information protection policies, as of February 2026.

If you have any questions about this Privacy Notice, please contact Technology Support and/or the Compliance department.

Appendix 1 - Lawful Grounds for processing Personal Data

Reason for Processing	Types of HR Personal Data	Basis for Processing
Making a decision about your recruitment or appointment.	Your personal details (including name, address, contact information); covering letters; CV/resume data*; references in; passport; visa; interview notes; suitability assessments	Legitimate interests: recruitment decisions
(Where appropriate) we may use information about criminal convictions to make a decision about your recruitment, appointment or promotion.	Information about criminal convictions	Compliance with a legal and/or FCA-regulatory obligation Legitimate interests: public interest, protecting our business and people, network and information security, preventing improper use of systems, protecting workforce Explicit consent
Determining the terms on which you work for us.	References; CV/resume data; interview notes; recruitment records; tax information; location, (potential) job title	Necessary for performance of the contract Legitimate interests: Attracting and retaining staff

Checking you are legally entitled to work in the UK.	Documentation required under immigration law; meeting/interview notes	Compliance with a legal obligation: right to work
Administering the contract we have entered into with you and operating our working relationship with you.	Name; bank account details; compensation information; social security number; tax information; benefits and expenses records; details of next of kin and benefits beneficiaries; time and attendance records; contact details for next of kin/emergency contact	Necessary for performance of the contract Legitimate interests: Operation of the employment relationship/engagement
Paying you and, if you are an employee, deducting tax and National Insurance contributions.	Name; IDs relating to payroll processing; bank account details; compensation information; social security number; benefits and expenses records; tax information; student loan information	Compliance with a legal obligation Necessary for performance of the contract
Providing benefits to you	Name; bank account details and financial information; social security number; benefits and expenses records; contact details for next of kin and benefits beneficiaries; tax information	Necessary for performance of the contract
Liaising with your pension provider	Name; bank account details and financial information; social security number; contact details for next of kin and benefits beneficiaries	Necessary for performance of the contract Compliance with a legal obligation
Business management and planning, including accounting and auditing.	Financial information; benefits and expenses records	Legitimate interests: business management and controls Compliance with legal obligation

Conducting performance reviews, managing performance and determining performance requirements, performance awards	Appraisal forms; interview and meeting notes; performance and development records; time and attendance records	Necessary for performance of the contract Legitimate interests: attracting and retaining talent; effective business operations
Making decisions about salary reviews and compensation.	Name; pay details; appraisal forms; bank details and financial information; benefits and expenses records; interview or meeting notes; performance and development records; time and attendance records	Necessary for performance of the contract
Assessing qualifications for a particular job or task, including decisions about promotions.	Name; CV/Resume data; performance reviews; interview or meeting notes; performance and development records; time and attendance records	Necessary for performance of the contract
In connection with grievance, disciplinary or capability hearings.	Time and attendance records; performance reviews; disciplinary records; appraisal forms; interview notes; performance and development records; disciplinary and grievance records; time and attendance records	Legitimate interests: Dealing with internal processes; management of workforce
Making decisions about your continued employment or engagement.	Time and attendance records; performance reviews; disciplinary and grievance records; appraisal forms; court, tribunal or inquiry proceedings; interview or meeting notes; performance and development records; time and attendance records	Legitimate interests: Management of workforce and effective business operations

Making arrangements for the termination of our working relationship.	Name; pay details; bank details and financial information; benefits and expenses records; interview or meeting notes/references out	Legitimate interests: Management of workforce and effective business operations
Education, training and development requirements (including quality improvement).	Appraisal forms; interview or meeting notes; performance and development records; disciplinary and grievance records; training records	Legitimate interests: Staff training and development; effective business operations
Dealing with legal disputes involving you, or other staff or third parties, including accidents at work.	Names; medical and health related information; checks; occupational health data; accident records; appraisal forms; court, tribunal or inquiry proceedings; interview notes; performance and development records; disciplinary and grievance records; time and attendance records	Legitimate interests: Responding to and defending legal disputes/claims; managing our risks
Ascertaining your fitness to work and occupational health.	Names; medical and health related information; checks; occupational health data; accident records; interview or meeting notes; time and attendance records	Compliance with a legal obligation: health and safety Performance of contract Legitimate interests: Management of workforce and effective business operations

Managing sickness absence.	Names; medical and health related information; checks; occupational health data; accident records; interview or meeting notes; time and attendance records	Compliance with a legal obligation Performance of employment contract Legitimate interests: management of absent employees/dealing with capability issues
Paying sick pay	Names; medical and health related information; checks; occupational health data; accident records; bank details and financial information; time and attendance records; tax information	Compliance with a legal obligation: payment and administration of sick pay Performance of employment contract
Arrangements relating to family related leave (for example: maternity, paternity, adoption, shared parental leave).	Names; dependents' details; service period; financial information; bank details; medical and health related information; co-parent's details	Compliance with a legal obligation: payment and administration of family related leave Performance of employment contract
Complying with health and safety obligations and health and safety records and management.	Medical and health related information; medical checks; occupational health data; accident records; interview notes; time and attendance records	Compliance with a legal obligation
Expenses reimbursement	Travel and expenses records	Necessary for performance of the contract

To prevent fraud.	Bank details and financial information; benefits and expenses records	Compliance with a legal obligation Legitimate interests: Fraud prevention and proper conduct of our business
To monitor your use of our information and communication systems to ensure compliance with our IT policies.	Emails in and out; recorded telephone calls	Compliance with a legal obligation Legitimate interests: network and information security, preventing improper use of systems, protecting workforce
To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution.	E-mails in and out; network use	Legitimate interests: ensuring system and data security
Whistleblowing procedures	Meeting notes; hearing records; investigation records	Legal obligations Legitimate interests: public interest, protecting our business and people

*CV/Resume data includes name, personal address, personal telephone, e-mail address, date of birth, age, government I.D, citizenship status, academic record or qualifications/skills/accreditations/career history.

8. UPDATES TO THIS GLOBAL PRIVACY NOTICE

ICONIQ Capital reserves the right to update or modify this Global Privacy Notice from time to time to reflect changes in our privacy practices, legal requirements, or business operations. Any material changes to this Global Privacy Notice will be communicated to employees and candidates through appropriate channels, which may include direct notification, posting on our internal systems, posting on our website(s) or other reasonable means.

We encourage you to review this Global Privacy Notice periodically to stay informed about how we protect and handle your personal information.

9. CONTACT INFORMATION

If you have any questions, concerns, or requests regarding this Global Privacy Notice or our privacy practices, please contact us using the jurisdiction-specific contact information provided in Sections 4, 5, 6, and 7 above, or use the following general contact details:

ICONIQ Capital Email: legalnotices@iconiqcapital.com

For jurisdiction-specific enquiries, please refer to the contact information provided in the relevant jurisdiction-specific section of this Global Privacy Notice.