

CAREER PRIVACY POLICY

Effective Date: September 5, 2025 (in accordance to Clause 11)

At IUX, we respect your privacy and are committed to protecting your personal data throughout the recruitment process. This Privacy Policy explains how we collect, use, store, share, and protect your personal information when you visit our Careers page or apply for a position with us. By accessing our Careers website or submitting your application, you agree to the terms set out in this Policy.

This Policy applies specifically to personal data submitted for recruitment purposes and is designed to ensure transparency and compliance with applicable data protection laws, including but not limited to the Personal Data Protection Act (PDPA) and, where applicable, the General Data Protection Regulation (GDPR).

1. Purpose of this Policy

The purpose of this Privacy Policy is to provide full transparency regarding the collection and use of personal data in relation to our recruitment activities. At IUX, we recognize the importance of respecting and protecting the privacy of individuals who express interest in joining our organization, whether by browsing our Careers page or submitting a job application. This Policy is intended to help you understand what personal data we collect, why we collect it, how we use it, with whom we may share it, and how we protect it.

We are committed to handling personal data in a manner that is fair, lawful, and responsible. The protection of your privacy is an essential aspect of our recruitment process and broader data governance strategy. By providing this Career Privacy Policy, we aim to ensure that you are fully informed of your rights and our obligations in relation to your personal data. We also wish to promote trust and accountability by setting out clearly the procedures we follow to ensure

your information is kept safe, processed with purpose, and retained only for as long as necessary.

This Policy applies exclusively to personal data collected through the Careers section of our website or otherwise provided by applicants for employment purposes, including through third-party platforms that we may use for candidate sourcing, application tracking, or interview scheduling. It does not apply to personal data collected in the context of other relationships with our organization, such as customers, vendors, or employees who have already joined us, which are governed by separate policies.

2. Types of Personal Data We Collect

We collect personal data from you directly when you submit an application, as well as automatically when you access our website. The personal data you provide may include, but is not limited to:

- full name,
- date of birth,
- email address,
- telephone number,
- residential address,
- resume or CV,
- cover letter,
- academic transcripts,
- educational history,
- professional certifications,
- employment history,
- salary expectations,

- and any other information you voluntarily submit during the recruitment process.

We may also collect data generated through your interaction with our Careers website, including technical and browsing data such as:

- IP address,
- browser type,
- operating system,
- language settings,
- access times,
- referring URLs,
- and device identifiers.

This data is typically collected through cookies or similar technologies, in accordance with our separate Cookie Policy if available. These technologies help us to understand user behavior, improve website functionality, and ensure a secure and consistent user experience.

In certain instances, and where permitted by applicable laws, we may collect sensitive or additional information relevant to the hiring decision. This may include results from pre-employment assessments or tests, notes from interviews, criminal background checks, identity verification documents, immigration status, CCTV footage from onsite interviews, and publicly available data from professional networking platforms (e.g., LinkedIn) or recruitment service providers. We may also collect audiovisual data, such as recordings from virtual interviews or recruitment events. When necessary, we will inform you in advance and obtain your explicit consent for the processing of any sensitive or non-standard categories of data.

If you participate in speaking engagements, online seminars, company-sponsored events, or marketing campaigns, we may collect additional information such as photographs, video footage, audio recordings, and your professional biography. This data may be used internally or externally in accordance with your consent and applicable data protection standards.

We make every effort to ensure that the personal data we collect is relevant, limited to what is necessary for recruitment purposes, and obtained through lawful and transparent means.

3. How We Use Your Personal Data

We process your personal data to facilitate and manage our recruitment and hiring operations. This includes evaluating your qualifications, work history, education, and suitability for current or future roles within our organization. The data you provide enables us to review your application materials, administer tests and interviews, coordinate with hiring teams, and communicate with you throughout the hiring process.

We may also use your data to verify your identity, check references, conduct background screening (where legally permitted), and ensure compliance with internal policies and external regulations. If you are invited to attend interviews or recruitment events, your data may be used for logistical coordination and internal reporting, and if consented, your participation may be documented through photographs or recordings.

In some cases, where you are not immediately selected for a role, we may retain your application and contact details to consider you for future positions that align with your profile. This proactive approach allows us to build a strong talent pool and reach out to potential candidates when new opportunities arise. Your data

may also be aggregated (in anonymized form) to help improve our recruitment strategies, assess the effectiveness of hiring campaigns, and identify areas for process improvement.

We do not use your data to send you general marketing communications unrelated to recruitment, nor do we sell your data to any third party. All use of your personal data is limited to the legitimate and clearly defined purposes outlined in this Policy and complies with applicable laws and regulations.

4. Legal Basis for Processing

Our processing of your personal data is carried out in accordance with applicable data protection laws and is based on one or more lawful grounds, depending on the nature of the personal data and the context in which it is collected. These legal bases ensure that our handling of your data is lawful, fair, and transparent.

Firstly, we may process your data based on your explicit consent. For example, if we require sensitive personal data (such as background checks or recordings of interviews), we will request your consent before proceeding. You have the right to withdraw this consent at any time by contacting us using the details provided in this Policy. Please note that the withdrawal of consent does not affect the lawfulness of any processing conducted prior to such withdrawal.

Secondly, much of our data processing is necessary for the purpose of taking steps at your request prior to entering into a contract. This includes reviewing your application, arranging interviews, assessing your qualifications, and making hiring decisions. Without this data, we would be unable to evaluate your suitability for employment.

Thirdly, we rely on our legitimate interests in conducting a fair, efficient, and secure recruitment process. This includes maintaining records for internal accountability, enhancing the quality of our hiring practices, preventing fraud, and defending against legal claims. When we process your data on this basis, we carefully balance our interests with your fundamental rights and freedoms, and we implement safeguards to protect your privacy.

In certain circumstances, we may also process your data to comply with legal or regulatory obligations, such as verifying your right to work, responding to government inquiries, or fulfilling audit and reporting requirements imposed by labor or data protection authorities.

Where our processing activities involve data transfers across borders, we ensure that additional legal mechanisms are in place to guarantee that your data is handled in compliance with the applicable international standards.

Overall, we are committed to processing your personal data only for clearly defined, lawful purposes and to maintaining full compliance with all applicable privacy and data protection legislation.

5. Sharing of Personal Data

We treat the confidentiality and integrity of your personal data with the utmost seriousness and do not sell, rent, or trade your personal information to any third party for commercial gain. However, to facilitate a transparent and effective recruitment process, we may share your data under specific conditions and only with trusted recipients who are contractually bound to process your data in accordance with applicable privacy laws and this Career Privacy Policy.

Access to your personal data is strictly limited to those who require it to fulfill legitimate recruitment-related functions. This includes members of our Human Resources team, internal recruiters, hiring managers, interview panel members, and, where necessary, our legal and compliance departments. Each of these individuals is required to maintain strict confidentiality and process your data solely for the purposes outlined in this Policy.

We may also share your data with third-party service providers that assist us in managing various aspects of the recruitment process. These may include vendors providing applicant tracking systems, background check services, psychometric or technical assessment tools, online interview platforms, and recruitment or executive search firms acting on our behalf. In all such cases, these providers are required to enter into data processing agreements with us, which include strict obligations regarding the security, use, and confidentiality of your information.

In limited circumstances, we may disclose personal data to public authorities, regulatory bodies, law enforcement agencies, courts, or legal counsel if we are required to do so by law, subpoena, regulation, or legal process. Such disclosure may also occur where necessary to exercise or defend our legal rights or those of our employees, contractors, or affiliates.

If your personal data is transferred to another entity as part of a merger, acquisition, restructuring, or similar corporate transaction, we will ensure that the recipient is bound by privacy obligations no less protective than those set forth in this Policy.

In all cases, we ensure that data sharing is minimized and restricted to only what is necessary and proportionate to achieve the intended and lawful purpose. We

will never authorize any party to use your data for purposes outside of the scope of recruitment, compliance, or as required by law.

If you have concerns about the parties with whom your data may be shared or wish to obtain further details about specific processors or categories of recipients, you may contact us using the details provided in Section 10 of this Policy.

6. International Data Transfers

Your personal data may be stored, accessed, or processed in countries outside of your country of residence, including in jurisdictions that may not provide the same level of data protection as those within your home country or region. Such transfers typically occur when we rely on international third-party service providers for the operation of our applicant tracking systems, background screening vendors, cloud storage providers, or online assessment platforms. These vendors may have servers or processing facilities located in jurisdictions such as the European Union, the United States, or countries in the Asia-Pacific region.

Whenever we transfer personal data internationally, we do so in strict accordance with applicable data protection laws and take appropriate measures to safeguard your information. Where required by law, we implement legally recognized mechanisms such as Standard Contractual Clauses (SCCs) approved by relevant supervisory authorities, Binding Corporate Rules (BCRs), or rely on adequacy decisions issued by competent regulators. These legal safeguards ensure that your personal data continues to benefit from a level of protection equivalent to that required in your country of residence.

Additionally, we evaluate the legal and regulatory frameworks of destination countries and conduct transfer impact assessments where necessary to identify and mitigate any potential risks to the rights and freedoms of data subjects. We also ensure that any international data recipient agrees to confidentiality obligations and appropriate technical and organizational measures, including limitations on access, processing purposes, and retention.

If you would like further information about the safeguards we implement for international data transfers or wish to receive a copy of the relevant Standard Contractual Clauses or similar arrangements, you may contact us using the details provided in Section 10 of this Policy.

We remain committed to upholding your privacy and ensuring that your personal data is protected, regardless of where it is processed.

7. Data Retention

We retain personal data of applicants for a period of one (1) to two (2) years from the date of submission, last communication, or final decision regarding the application process, whichever is later. This retention period allows us to assess candidate suitability for future roles, to respond to follow-up inquiries or regulatory matters, and to fulfill our legitimate interest in maintaining a historical record of recruitment activity.

If your application is successful and you become employed by us, your personal data will be retained as part of your employee record and governed under a separate employee privacy notice or internal data protection policy. If your

application is unsuccessful, your data will be stored for the duration specified above unless you request its earlier deletion.

There may be instances where we are required by law, regulation, or internal audit purposes to retain your data for longer periods. For example, if your application or assessment results are subject to legal claims, investigations, or compliance reviews, we may retain relevant information beyond the standard retention period. In such cases, your data will be securely archived and access will be restricted to authorized personnel on a strict need-to-know basis.

Where applicable, we may also anonymize your data after the initial retention period. Anonymized data may be used for research, recruitment analytics, diversity monitoring, and to improve our talent acquisition strategies.

Anonymization is conducted in such a way that you are no longer identifiable and the data is no longer considered "personal data" under applicable privacy laws.

You may request deletion of your personal data at any time by contacting us via the contact details provided in Section 10. However, please note that we may be required to retain certain data for a minimum duration as required under local employment or data protection legislation. All requests for data deletion will be assessed and responded to in accordance with our legal obligations and internal data handling procedures.

8. Security of Your Information

We take the security of your personal data seriously and are committed to implementing and maintaining appropriate technical and organizational measures to safeguard it against unauthorized access, loss, misuse, alteration, destruction,

or disclosure. Our security framework is designed to ensure the ongoing confidentiality, integrity, and availability of personal data throughout its lifecycle.

To this end, we implement a range of physical, administrative, and technological safeguards. These include, but are not limited to, access control mechanisms that restrict data access only to authorized personnel on a need-to-know basis, secure and encrypted data storage solutions, firewalls, anti-virus protection, and secure transmission protocols such as HTTPS. We also maintain robust internal policies and procedures governing data handling and processing, which all staff members are trained to follow.

Additionally, we routinely monitor our systems for potential vulnerabilities and engage in periodic audits, risk assessments, and penetration testing to evaluate the effectiveness of our controls. When we engage third-party service providers to process personal data on our behalf, we ensure that they are contractually bound to adhere to security standards that are no less protective than those we apply ourselves.

In the unlikely event of a data breach that poses a risk to your rights and freedoms, we will promptly investigate the incident, take all necessary remedial actions, and, where legally required, notify the relevant supervisory authority and affected individuals in accordance with applicable data protection laws. We also maintain an internal incident response procedure to ensure that such events are handled swiftly and transparently.

While no system or method of transmission over the internet can be guaranteed to be 100% secure, we continuously strive to enhance our security posture in line

with industry standards and emerging best practices to protect your personal data to the fullest extent possible.

9. Your Rights

As a data subject, you have a number of rights in relation to your personal data, subject to the applicable data protection laws in your jurisdiction. These rights are designed to give you transparency and control over how your personal data is collected, used, and retained by us. We are committed to facilitating the exercise of these rights in a fair and timely manner.

You have the right to access your personal data. This means you may request confirmation as to whether or not we process your personal data, and where that is the case, obtain a copy of the personal data we hold about you, together with information about how and why it is processed.

You have the right to rectification, allowing you to request that inaccurate or incomplete personal data be corrected or updated. We encourage applicants to inform us promptly of any changes to their information to ensure accuracy throughout the recruitment process.

You also have the right to erasure, sometimes referred to as the “right to be forgotten.” This permits you to request the deletion of your personal data where, for example, the data is no longer necessary for the purpose for which it was collected, or where you have withdrawn your consent (where consent was the legal basis), or where the processing is no longer lawful. Please note that we may retain certain data where required by law or to establish, exercise, or defend legal claims.

You have the right to object to our processing of your personal data in certain situations, including where processing is based on our legitimate interests and you believe that such processing has an unjustified impact on your fundamental rights and freedoms. If you object, we will cease processing your data unless we can demonstrate compelling legitimate grounds to continue.

In some cases, you may exercise your right to restriction of processing, which allows you to request that we temporarily suspend the processing of your personal data under specific conditions—such as while the accuracy of the data is being verified, or where you have objected to processing and we are considering whether our legitimate grounds override yours.

Where we rely on your consent to process your personal data, you have the right to withdraw that consent at any time. This withdrawal will not affect the lawfulness of processing based on consent before its withdrawal, but it may affect our ability to continue the recruitment process with you.

Depending on the jurisdiction and circumstances, you may also have a right to data portability, meaning that you can request to receive your personal data in a structured, commonly used, and machine-readable format, and request that such data be transmitted directly to another controller where technically feasible.

If you believe that we have failed to respect your data protection rights, you also have the right to lodge a complaint with a data protection supervisory authority. While we would appreciate the opportunity to address your concerns directly, you are entitled to contact the relevant authority at any time.

To exercise any of the rights outlined above, please contact us using the contact details provided in Clause 10 of this Policy. We may request verification of your identity before we are able to process your request. We will respond to all legitimate requests within a reasonable timeframe, and in accordance with applicable legal requirements.

10. Contact Us

If you have any questions, concerns, or requests regarding this Career Privacy Policy or your personal data, you may contact us at:

Email: career@iux.com

We will endeavor to respond to your inquiry promptly and in accordance with applicable laws.

11. Updates to This Policy

We reserve the right to update or modify this Career Privacy Policy at any time in order to reflect changes in our recruitment practices, applicable laws, technological developments, or the way we manage personal data. We are committed to ensuring that our applicants are informed of how their personal data is handled, and we take privacy transparency seriously.

All updates will be published on this page with a revised “Effective Date” indicated at the top of the document. In cases where the changes materially affect the way we collect, use, or share your personal data—especially in ways that differ from what was originally communicated to you—we will make reasonable efforts to notify you in advance, where required by law. Such notifications may be delivered

via email (if we have your contact details), or prominently displayed on our website.

We encourage you to review this Policy periodically, especially before submitting a new application or engaging with our Careers platform. Your continued use of the site or submission of personal data following the publication of updates constitutes your acknowledgment and agreement to the revised terms.

If you do not agree with any part of the revised Policy, you should contact us to withdraw your application or exercise your rights as described in Section 9 of this Policy. For questions about the content of any version of this Policy, or to request a copy of a previous version, please contact our Data Protection Officer using the contact details provided in Section 10.

12. Cookie Notice

When you visit our Careers website or access our online application portal, we may use cookies and similar tracking technologies to enhance your browsing experience, analyze site performance, and better understand how visitors engage with our content. This clause explains how these technologies operate, the categories of data they collect, and your rights in relation to them.

Cookies are small data files that are stored on your device (computer, mobile phone, tablet, etc.) when you visit a website. They enable us to recognize your browser or device, remember your preferences, and provide certain functionalities. Some cookies are set directly by us (“first-party cookies”), while others may be set by third-party service providers that support our website features or analytics (“third-party cookies”).

We use both session cookies, which expire once you close your browser, and persistent cookies, which remain on your device for a specified period or until you delete them. The types of cookies we may use include:

- **Strictly Necessary Cookies:** These are essential for the proper functioning of our website and for enabling core services such as secure login, application submission, and navigation. Without these cookies, certain parts of the site may not function correctly.
- **Performance and Analytics Cookies:** These cookies collect information about how visitors use our Careers site, such as which pages are visited most frequently or whether users encounter errors. The data collected is aggregated and used to improve the site's performance and user experience. We may use tools such as Google Analytics or similar platforms for this purpose.
- **Functional Cookies:** These cookies allow the website to remember choices you make, such as your preferred language or region, and provide more personalized features.
- **Security Cookies:** These cookies help us detect and prevent potential security threats and unauthorized access to our systems.

Depending on your location and applicable data protection laws, we may request your consent before placing non-essential cookies on your device. Where required, a cookie banner or settings panel will be presented to you upon visiting the site, allowing you to accept or reject specific cookie categories.

You can manage or delete cookies at any time through your browser settings. Most web browsers allow you to control cookies through their settings preferences. However, please note that disabling certain cookies may impact your ability to access or use some features of our Careers site.

If a separate Cookie Policy is implemented, we will provide a prominent link to that policy on the website, which will offer a more detailed description of cookie types, duration, and how to manage your preferences.

By continuing to use our Careers website without changing your cookie settings, you consent to our use of cookies and similar technologies as described in this Policy.