PRIVACY NOTICE FOR CANDIDATES AND PROSPECTIVE EMPLOYEES OF THE INTO COMPANIES AND ASSOCIATED JOINT VENTURES

October 2024

Contents

About this Privacy Notice

This privacy notice is issued by the following companies which are referred to in this document as “The Companies”.

In the United Kingdom:

- INTO City LLP
- INTO Lancaster Ltd
- INTO London MDX Street LLP
- INTO London World Education Centre Ltd
- INTO Manchester Ltd
- INTO Newcastle University LLP
- INTO Queens LLP
- INTO UEA LLP
- INTO University of Exeter LLP
- INTO University of Stirling LLP
- INTO University Partnerships Ltd
- IUP2 LLP
- Delta Language and Training Consultancy Ltd (trading as NILE)

In the United States of America:

- INTO Long Island, LLC
- INTO Mason, LLC
- INTO North America, Inc.
- INTO NY at Drew, LLC
- INTO OSU, Inc.
- INTO SLU, LLC
- INTO Suffolk, LLC
- INTO UAB, LLC

Outside the UK and US:

- IUP (Asia) Ltd (Topco)
- IUP Asia Ltd
- INTO Australia Pty Ltd
- INTO China Ltd (WFOE)
- INTO Education India Private Ltd
- INTO Global MENA FZ LLC
- INTO (Malaysia) Sdn. Bhd
- INTO Perth Pty Ltd
- DPU (Shanghai) Business Consulting Ltd
- Guangzhou INTO Education Information Consulting Co. Ltd
- PT INTO Global Indonesia
- UAC Kazakhstan LLP
- UAC Vietnam Ltd
- University Access Centre (Thailand) Co. Ltd
- University Access Centre SAS

Introduction

In this privacy notice, the terms "we", "our", and "us" refer to The Companies listed above.

Each of The Companies is a controller of your personal information, which means that we are responsible for looking after it. We will use your personal information fairly, lawfully and in a transparent manner, and in accordance with the Data Protection Laws in the multiple jurisdictions that INTO operates globally.

This privacy notice describes how we collect and use personal information about you while you are applying to work with us, either as an employee or contractor. This notice does not form part of any contract of employment or other contract to provide services.

It is important that you read this privacy notice, together with the supplementary privacy notices we provide for people resident in Australia, China, or U.S.A., or other fair processing notices provided on specific occasions when collecting or processing personal information about you, so that you are fully aware of how and why we are using such information. This privacy notice supplements the other notices and is not intended to override them.

If you have any questions in relation to this notice or how your personal information is processed, please contact our Data Protection Officer by email at: privacy@intoglobal.com

What do the key terms mean?

"Data Protection Laws" means (a) to the extent the UK GDPR and Data Protection Act 2018 applies, as laws of the United Kingdom which relate to the protection of individuals when processing their personal information; and (b) to the extent the EU GDPR applies, the law of the European Union or any member state of the European Union which relates to the protection of individuals with regards to the processing of personal information; and (c) relevant data protection laws in other jurisdictions where the Companies (on page 3) are based, for example China's Personal Information Protection Law (PIPL) and the Australian Privacy Principles that form the Privacy Act 1988.

"Personal information" means any information which we hold about you from which you can be identified. It may include contact details, identification numbers, other personal information, photographs, expressions of opinion about you or indications as to our intentions about you. Personal information does not include data where the identity has been removed (anonymous data).

"Processing" (and "Process" or "Processed") means doing anything with the personal information, such as collecting, recording, organising, structuring, storing, adapting or altering, retrieving, accessing, consulting, disclosing, disseminating, aligning or combining, restricting, erasing or destroying, or using the data in any way.

The information we collect about you

When you apply to work with us, we may collect, store, use and transfer different kinds of personal information about you which we have grouped together as follows:

- **Identity Information** includes first name, previous last name, current last name, username or similar identifier, marital status, title, date of birth, gender, dependants (USA only), and images such as photographs and videos.
- **Contact Information** includes home address, telephone numbers, personal email address, next of kin and emergency contact information.
- **Compliance Information** includes National Insurance / Social Security number, copy of driving licence and passport, and for relevant posts, results of enquiries to the UK Disclosure and Barring service or local equivalent in other countries.
- **Recruitment Information** includes copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process, results of reference requests, statutory eligibility to work verification, and personal information you provide to us or questions you ask us during an interview,whether conducted in person, by telephone or by video conferencing.

How your personal information is collected

We may collect personal information about candidates from the following sources:

- You, the candidate;
- Any recruitment agency appointed by you or us;
- Any appointed background check provider or similar government agency (US only);
- For certain roles and locations, any credit or other referencing agency;
- Criminal records checking service (DBS in the UK) in respect of criminal convictions;
- Reference providers;
- Publicly available information including LinkedIn and other social media sites.

How we will use your personal information

We will use your personal information to:

- Objectively assess your skills, qualifications, and suitability for the role applied for;
- Safeguarding checks, including background, identity and reference checks, where applicable;
- Communicate with you about the recruitment process;
- Keep records related to our recruitment processes;
- Comply with legal or regulatory requirements;
- Perform statistical analysis (although this data will be anonymised).

It is in our legitimate interests to decide whether to appoint you to the role applied for since it would be beneficial to our business to appoint someone to that role and we need to process your personal information to decide whether to make an offer of employment to you.

We will use information about you during the recruitment process to make decisions regarding suitability for shortlist, interviewing, reference checking, offer and appointment.

If you fail to provide personal information

If you fail to provide certain information when requested, which is necessary for us to consider your application(such as evidence of qualifications or work history), we will not be able to process your application. For example, if we require a check of your criminal records (known as a DBS check in England and Wales; a Disclosure Request in Scotland; or Access NI in Northern Ireland), a pre-employment credit check or references for a particular role and you fail to provide us with relevant details, we will not be able to take your application further.

Special Category Data

We may hold information about you which is classified as 'special category data' or ‘sensitive personal information’ within the Data Protection Laws, such as details about your ethnicity and racial or ethnic origin, your health, any disabilities, and data relating to any criminal (or alleged criminal) offences or convictions, which you have supplied to us.

We will only process this special category data in circumstances where you have given your explicit consent, where it is legally required, where it is necessary for us to meet our obligations or exercise our rights as an employer, where there is a substantial public interest in doing so, or where you have already made the data public. We set out more detail in relation to this processing in our Special Category and Criminal Offence Data Policy which you can read here.

We may also use your special category data in the following ways:

- for the purposes of equal opportunities monitoring and reporting when information about your nationality or ethnic origin will be used;
- to make any reasonable adjustments that may be needed during the recruitment process that are requested by you (the candidate), for example whether adjustments need to be made during a test or interview to meet accessibility needs;
- to meet our obligations under the Fair Employment and Treatment regulations for candidates based in Northern Ireland;
- to use temperature testing to ensure the safety of our sites in the context of a pandemic.

To comply with PIPL, applicants resident in mainland China will be asked to consent to their sensitive personal information being processed as set out above. We will provide you with specific details of the processing at the point at which your consent is collected during the recruitment process and the reason why your consent is needed.

Information about Criminal Convictions

We will only use information relating to criminal convictions where permitted to do so by the Data Protection Laws and then only in accordance with our Special Category and Criminal Offence Data Policy which you can read here. Processing of criminal conviction data occurs when it is necessary for us to comply with the law or for another reason where there is a substantial public interest in us doing so, for example, in relation to safeguarding of students or similar.

Where appropriate, we will use information relating to criminal convictions or alleged criminal behaviour in relation to legal claims, where it is necessary to protect your interests, or someone else's interests and you are not capable of giving your consent, or where you have already made the information public.

For certain roles we are required and/or entitled to carry out a criminal records check to satisfy ourselvesthat there is nothing in your criminal convictions history which makes you unsuitable. In particular:

- We are required by law to carry out criminal record checks for those carrying out teachingand other roles where there may be unaccompanied contact with minors;
- Some roles, for example, senior roles in Finance, Human Resources and Legal require a high degree of trust and integrity and so we may ask you to seek a basic disclosure of your criminal records history.

Automated decision-making

You will not be subject to decisions that will have an impact on your application based solely on automated decision-making (ADM). ADM typically takes place when an electronic system uses personal information to make a decision without human intervention. We are allowed to use automated decision-making in the following circumstances:

- Where we have notified you of the decision and given you 21 days to request a reconsideration.
- Where it is necessary to perform the contract with you and appropriate measures are in place to safeguard your rights.
- In limited circumstances, with your explicit written consent and where appropriate measures are in place to safeguard your rights.

Data Sharing

We may share your personal information with credit checking, other referencing agencies and recruitment agencies for the purposes of processing your application. All our third-party service providers and other entities in the INTO Group are required to take appropriate security measures to protect your personal information in line with our policies.

We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

There are some roles where the recruitment process includes employees of our partner universities and INTO Companies other than the one you have applied to. In these cases we will share your personal and relevant sensitive personal information with those specific employees solely for the purposes of the recruitment process.

To comply with PIPL, applicants who are resident in mainland China will be asked to consent to their personal information being provided with any or all of our third-party personal information processors. We will provide you with details of the processing at the point at which your consent is collected and the reason why your consent is needed.

International Data Transfers

Personal information submitted during recruitment may be held in the country where the vacancy is based and also be available to INTO's Head Office in the UK; it may also be transferred to another country where our systems or data stores are hosted.

For applicants in the Asia Pacific region, we will also transfer personal information to China and Hong Kong as this is where our regional HR offices are located.

For applicants resident in mainland China, your personal information will be processed in accordance with applicable personal information privacy laws in China, including the Personal Information Protection Law of China (PIPL), as set out in our supplementary Privacy Notice for China. You will also be asked to consent to the transfer of documents and files containing their personal information outside of China to comply with PIPL. These transferred documents and files will be those necessary for INTO's UK Head Office to have access to in order to fulfil any or all of the Purposes shown on page 5.

Such data transfers are covered by the safeguards and data protection standards put in place and documented in INTO's Intra-Group International Data Transfer Agreement, and the Standard Contract for Outbound Cross-border Transfer of Personal Information to comply with PIPL.

Information Security

We place great importance on the steps we take, including use of different technologies and physical and organisational measures, to protect your personal information from unauthorised access and against unlawful processing, accidental loss, alteration, disclosure, destruction and damage.

We have procedures and technologies in place to maintain the security of personal information from the point of collection to the point of destruction. We will only transfer your personal data to third parties if they agree to comply with those procedures and policies, or if they put in place adequate measures themselves.

Further details may be obtained from our Data Protection Officer via email: privacy@intoglobal.com

Information Retention

We will keep your personal information for a period of twelve months after we have communicated our decision to you about whether to appoint you to the role applied for. We retain your personal information for that period so that we can show, in the event of a legal claim, that we have not discriminated against candidates on prohibited grounds and that we have conducted the recruitment exercise in a fair and transparent way. After this period, we will securely destroy your personal information in accordance with our data retention policy or applicable laws and regulations.

If we wish to retain your personal information on file, on the basis that a further opportunity may arise in future and we may wish to consider you for that, we will write to you separately, seeking your explicit consent to retain your personal information for a fixed period on that basis.

Rights of access, correction, erasure and restriction

You have a number of legal rights in relation to your personal information under Data Protection Laws, including the Right to be Informed, which is why we provide you with clear and concise information about what how your personal information is used via this privacy notice, as well as the right to:

- **Request access to your personal information** (commonly known as a "data subject access request"). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it;

- **Request correction of the personal information that we hold about you.** This enables you to have any incomplete or inaccurate information we hold about you corrected;
- **Request erasure of your personal information.** This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also havethe right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below);
- **Object to processing of your personal information** where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes;
- **Request the restriction of processing of your personal information.** This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it;
- **Request the transfer of your personal information to another party.** We will provide to you, or a third party you have chosen, your personal data in a structured, commonly used, machine-readable format. Note that this right only applies to automated information which you initially provided consent for us to use; and
- **Withdraw your consent at any time where we are relying on consent to process your personal data.** When you applied for a role with one of The Companies, you provided consent for us to process your personal information for the purposes of the recruitment process. You have the right to withdraw your consent for processing for that purpose at any time. To withdraw your consent, please contact our Data Protection Officer using the details below. Once we have received notification that you have withdrawn your consent, we will no longer process your application and, subject to our data retention policy, we will dispose of your personal information securely.

If you wish to exercise any of your right as listed above, please contact our Data Protection Officer by completing our Online Rights' Request form or send an email to mailto:privacy@intoglobal.com

Time limit to respond

We aim to respond to all legitimate requests as soon as possible and within one calendar month of receipt. Occasionally it may take us longer than a month if your request is particularly complex or you have made a number of requests. In this case, we will notify you and keep you updated.

No fee usually required

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, in our view, your request for access is manifestly unfounded or excessive, or if you ask for further copies of your data.. Alternatively, we may refuse to comply with the request in such circumstances.

What we may need from you

We may need to request specific information from you to help us 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.

Contacting our Data Protection Officer

Please use our Online Rights' Request form or send an email to: privacy@intoglobal.com

Address: F.A.O. The Data Protection Officer, INTO University Partnerships Limited, One GloucesterPlace, Brighton, East Sussex, BN1 4AA, England.

Each of The Companies in the United Kingdom are subject to regulation by the UK's Information Commissioner's Office (the "ICO"). You can contact the ICO for adviceand support, however, we would really appreciate the opportunity to assist you at the outset if you have any queries regarding this notice or how we use your personal information.

Changes to this Privacy Notice

We reserve the right to update this privacy notice at any time.