

Recruitment Privacy Notice

DOCUMENT CLASSIFICATION	Level 0 – Unclassified
DOCUMENT REF	Comp/GDPR/PrivacyNotices/001
VERSION	1.0
DATED	17 August2023
DOCUMENT AUTHOR	CM
DOCUMENT REVIEW	16 08 2024

Revision history

VERSION	DATE	REVISION AUTHOR	SUMMARY OF CHANGES
0.1	17.08.2023	CM	Creation of Document
0.2	07.09.2023	GW	Minor edits from Recruitment

Distribution

NAME	TITLE
Unclassified – Public Domain	Recruitment Privacy Notice

Approval

NAME	POSITION	SIGNATURE	DATE
Dannii Darling	Compliance Manager and DPO	D.Darling	7.9.23

Recruitment privacy notice

The Institute of Export and International Trade is committed to protecting the privacy and security of your personal information.

This privacy notice describes how we collect and use personal information about you during the recruitment process, in accordance with the General Data Protection Regulation (GDPR) and applies to all candidates.

This Privacy Notice is for information only; it is not a contractual agreement.

This privacy notice applies across all entities or subsidiaries owned, controlled, or operated by the Institute of Export and International Trade or forming part of its Group and to all team members, including part-time, temporary, or contract team members or consultants or external contractors of the Institute of Export and International Trade. This Privacy Notice will also apply in the event that the Institute of Export and International Trade provides recruitment services for a Member Organisation.

What information do we collect?

In connection with your application for work with us or expression of interest in a vacancy which we have available, we will collect, store, and use the following categories of personal information about you:

The information you have provided to us in your curriculum vitae and covering letter/email/any correspondence between us;

Any information you provide to us during an interview; and

Information you provide in relation to your right to work documentation.

We may also collect, store and use the following “special categories” of more sensitive personal information:

Information about your health, including any medical condition, health and sickness records; and

Information about your criminal record.

We collect this personal information from the following sources:

- You, the candidate;
- Recruitment agencies;
- Search consultants;
- Our employment background check provider,
- Our credit reference agency;
- Your named referees; and
- Data from third party publicly accessible sources. For example, SRA and CILEx professional memberships.

In addition to us obtaining information from you directly as a data subject we may obtain information which is available in the public domain from various job sites / forums such as LinkedIn. When this is the case if we extract this data and process the data on our internal systems we will contact you to seek your explicit consent for us to store your data. If you do not respond to us with an affirmative action confirming you are content for us to store your data for the purposes of contacting you in relation to any vacancies which we believe may be of interest to you we confirm we will cleanse your data.

Why do we process personal data?

We need to your process data to take steps either at your request where you have contacted us in relation to a vacancy prior to considering your application. We also need to process your data to fulfil all parts of our recruitment process. Where we process data in response to a request from you this would be in order to fulfil legitimate interests between both parties – your interest in exploring a potential vacancy opportunity with ourselves and our legitimate interest in considering you for a vacancy.

Where we have obtained your data from a third party where your data is in the public domain as set out above we will contact you to seek your consent to process your data and to contact you in relation to any vacancy opportunities which we believe may be of interest to you.

In some cases, we need to process data to ensure that we are complying with our legal obligations. For example, we are required to check your eligibility to work in the UK before employment starts.

We have a legitimate interest in processing personal data during the recruitment process and for keeping records of the process. Processing data from you allows us to manage the recruitment process, assess and confirm your suitability for employment and decide to whom to offer a job. We may also need to process data from you to respond to and defend against legal claims.

We process health information if we need to make reasonable adjustments to the recruitment process for you. This is to carry out our obligations and exercise specific rights in relation to employment.

Where we process other special categories of data, such as information about ethnic origin, sexual orientation, health or religion or belief, this is for equal opportunities monitoring purposes.

We are entitled to carry out a criminal records check in order to satisfy ourselves that there is nothing in your criminal convictions history which makes you unsuitable for the role. We use a third party to do this on our behalf and may receive a copy of their report if you have consented for us to do so.

We will not use your data for any purpose other than the recruitment exercise for which you have applied.

Who has access to data?

Your information will be shared internally for the purposes of the recruitment exercise. This includes members of the HR and recruitment team, interviewers involved in the recruitment process, managers in the business area with a vacancy if access to the data is necessary for the performance of their roles. If you proceed to employment with ourselves then we may also share some of your personal detail with our outsourced third party IT provider in order to complete our new starter process.

We will not share your data with third parties, unless your application for employment is successful and we make you an offer of employment. We will then share your data with former employers to obtain references for you, our employment background check provider to obtain necessary background checks. All our third-party service providers are required to take appropriate security measures to protect your personal information in line with our policies.

In cases where the IoE&IT is assisting a member organisation with recruitment, we will make this very clear to you in person and secure your specific approval before sharing your information with that organisation.

We do not envisage transferring the personal information we collect about you outside the EU.

How do we protect data?

We take the security of your data seriously. We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal information to those team members and other third parties on a need to know basis. They will only process your personal information on our instructions and they are subject to a duty of confidentiality. In addition to this and as part of our commitment to information security and the protection of all of our information assets we can confirm we are accredited to ISO 27001.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator where applicable of a suspected breach where we are legally required to do so.

For how long do we keep data?

If your application for employment is unsuccessful, we will hold your data on file for 24 months after the end of the relevant recruitment process. After this period, we will securely destroy your personal information in accordance with our data retention policy.

If your application for employment is unsuccessful we will retain your personal information on file for 24 months, during which time we may contact you to give you the opportunity to become an active candidate for a future vacancy. After the end of the last relevant recruitment process, on the basis that a further opportunity may arise in future and we may wish to consider you for that vacancy. We would contact you on this basis believing it is in the legitimate interests of both parties as you have expressed an interest in working with us. Any correspondence that you receive from us will have our privacy notice and contact details attached to this email so that you can advise us if you do not wish for us to contact you with regards to any further opportunities which we legitimately believe will be of interest.

90 days before the expiry of that 24 month period we will write to you separately advising you seeking your explicit consent to retain your personal information for a further fixed period of 24 months should any further relevant vacancies which we believe may be of interest to you become available. If we do not receive your explicit consent to continue to contact you within those 90 days we confirm that your personal data will be securely destroyed and cleansed from our system.

The 24 months retention period where we may contact you about other vacancies which we believe you may be interested in will commence from your last relevant recruitment process.

For example if you have applied for two vacancies with us the end of the relevant recruitment process (and the start of the 24 month period) will be on the date the later of the two applications is advised as unsuccessful.

In addition if you apply for a vacancy six month after your first application and both did not proceed to employment then the relevant date would be the date we confirm that the later vacancy application was unsuccessful.

If your application for employment is successful, personal data gathered during the recruitment process will be transferred to your personnel file. The periods for which your data will be held will be provided to you in a new privacy notice.

Your rights

As a data subject, you have a number of rights. You can:

- access and obtain a copy of your data on request;
- require us to change incorrect or incomplete data;
- require us to delete or stop processing your data, for example where the data is no longer necessary for the purposes of processing;
- object to the processing of your data where we are relying on our legitimate interests as the legal ground for processing; and
- ask us to stop processing data for a period if data is inaccurate or there is a dispute about whether or not your interests override our legitimate grounds for processing data.

We have included a helpful link to the Information Commissioner's website should you wish to read about your rights as a data subject:- <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/individual-rights/>

If you would like to exercise any of these rights, you can of course make your request via any means to any Team Member, however we would request that you contact our DPO at Compliance@export.org.uk.

If you believe that we have not complied with your data protection rights, you can complain to the Information Commissioner. We have included their details below for your ease of reference:- <https://ico.org.uk/global/contact-us/>

What if you do not provide personal data?

You are under no statutory or contractual obligation to provide data to us during the recruitment process. However, if you do not provide the information, we may not be able to process your application properly or at all.

Automated decision-making

Currently we do not utilise automated decision making as part of our processing activities.

Changes to this Privacy Notice

We confirm that we will review this privacy notice periodically and where we require to do so we will update this privacy notice.

If you have any questions about this privacy notice, please contact our Data Protection Officer at Compliance@export.org.uk.