Job Applicant Privacy Notice

V6.1 April 2024

Contents

Job Applicant Privacy Notice.

Controller: IQUW Administration Services Limited, 30 Fenchurch Street, London EC3M 3BD

Data protection officer: Simon Mahaffey, Data Protection Officer, 30 Fenchurch Street, London EC3M 3BD,

E-mail: dpo@iquw.com

What is the purpose of this document?

IQUW Administration Services Limited (IQUW) is committed to protecting the privacy and security of your personal information.

You are being sent a copy of this privacy notice because you are applying for work with us (whether as an employee, worker, or contractor). This privacy notice describes how we collect and use personal information about you during the recruitment process, in accordance with the UK General Data Protection Regulation (UK GDPR).

IQUW is a 'controller.' This means that we are responsible for deciding how we hold and use personal information about you. This privacy notice describes the personal information we collect, why we need it and how we use it.

We may update this notice from time to time.

It is important that you read this notice so that you are aware of how and why we are using such information.

If you have any questions about this privacy notice or how we handle your personal information, please contact Simon Mahaffey, at the address and contact details above.

Data Protection Principles

We take our data protection responsibilities seriously and endeavour to comply with the Data Protection Act and other relevant law. We acknowledge that the personal information we hold about you must be:

1. Used lawfully, fairly and in a transparent way.
2. Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
3. Relevant to the purposes we have told you about and limited only to those purposes.
4. Accurate and kept up to date.
5. Kept only as long as necessary for the purposes we have told you about.
6. Kept securely.

The kind of information we hold about you.

Personal information means any information about an individual from which that person can be identified. There are 'special categories' of more sensitive personal data which require a higher level of protection, and these are described below.

We collect, store, and process a range of personal information about you. This may include:

- your name, title, address, and contact details, including email address and telephone number, and date of birth.
- details of your qualifications, skills, experience, and employment history, including start and end dates, with previous employers and with IQUW.
- details of your bank account and national insurance number.
- information about your entitlement to work in the UK.
- details of your contract (days of work and working hours).
- location of workplace.
- recruitment information (including copies of right to work documentation, references and other informationincluded in a CV or cover letter or as part of the application or interview process).
- CCTV footage, call recordings and other information related to our premises, such as building access card records.
- information about your use of our information and communications systems.
- next of kin and emergency contact details
- termination of contract

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

- Information about your health, disability, and any pre-existing medical conditions.
- Criminal records
- Information about your ethnic origin, nationality, gender, sexual orientation, marital status or religion or belief

How is your personal information collected?

The organisation collects this information in a variety of ways. For example, data might be contained in application forms, CVs or resumes, obtained from your passport or other identity documents, or collected through interviews or other forms of assessment, including online tests, and online forms. The organisation will also collect personal data about you from third parties, such as references supplied by former employers, information from employment background check providers and information from criminal records checks. The organisation will seek information from third parties and will inform you that it is doing so. The categories of data we collect from third parties are as follows:

Source	Category of data
Former employers	Employment references, details of experience and employment history, including start and end dates
Background check provider	Criminal convictions, Employment references, Gap verification, Adverse financial history, Identity verification, Highest qualification reference, Directorship search, FCA basic check.
Disclosure and Barring Service	Criminal convictions

Data will be stored in a range of different places, including on your application record, in HR management systems and on other IT systems (including email).

Why will we use information about you?

We will only use your personal information when the law allows us to, or with your consent if applicable law requires consent. Most commonly, we will use your personal information in the following circumstances:

1) Where we need it to take steps at your request prior to entering a contract with you, or to enter a contract with you.
2) Where we need it to comply with a legal obligation. For example, it is required to check a successful applicant's eligibility to work in the UK before employment starts.
3) Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests. We have a legitimate interest in processing personal data during the recruitment process and for keeping records of the process. Processing data from job applicants allows us to manage the recruitment process, assess and confirm a candidate's suitability for employment and decide to whom to offer a job.

We may also use your personal information in the following situations, which are likely to be rare:

1) Where we need to protect your vital interests (or someone else's vital interests), e.g., in a life-or-death situationor if there are critical injuries.
2) Where it is needed in the public interest or for official purposes.
3) We may also need to process data from job applicants to respond to and defend against legal claims.

The organisation will retain your personal information shared at your interview and/or contained within your interview pack for a period of 12 months after the organisation has communicated to you our decision about whether to appoint you to a role. The organisation retains your personal information for that period so that the organisation can show, in the event of a legal claim, that the organisation has not discriminated against candidates on prohibited grounds and that the organisation has conducted the recruitment exercise in a fair and transparent way. After this period, the organisation will securely destroy your personal information in accordance with applicable laws and regulations.

If your application is referred to the 'merit list,' the organisation will keep your personal data on file for a period of 12 months after the organisation has communicated to you our decision about whether to appoint you to a role. The 'merit list' will be used in the event there are future employment opportunities for which you may be suited. In this event, the organisation will ask for your consent before it keeps your data for this purpose, and you are free to withdraw your consent at any time by contacting careers@iquw.com

Occasionally your data may be kept on file for longer than the periods determined in this section should the organisation perceive a legitimate interest to do so, or if the organisation needs to do so to investigate or defend claims relating to the recruitment process.

Situations in which we will use your personal information.

We need all the categories of information in the list above primarily to allow us to decide whether to enter a contract with you and to enable us to comply with our legal obligations. It is also in our legitimate interests to process your personal information to decide whether to appoint you to a role since it would be beneficial to our business to appoint someone to that role. The situations in which we will process your personal information are listed below.

- Deciding about your appointment
- Assessing your suitability for work
- Determining the terms on which you work for us.
- Checking you are legally entitled to work in the UK.
- Carrying out background and reference checks
- Communicating with you about the recruitment process
- Business management and planning, including accounting and auditing.
- Dealing with legal disputes
- Ascertaining your fitness to work
- Complying with legal or regulatory requirements

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

Change of purpose.

We will only use your personal information for the purposes for which we collected it, unless we consider that we need to use it for any other reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

How we use particularly sensitive personal information.

"Special categories" of particularly sensitive personal information require higher levels of protection. We need to have further justification for collecting, storing, and using this type of personal information. We have in place an appropriate policy document and safeguards which we are required by law to maintain when processing such data. We may process special categories of personal information in the following circumstances:

1) We may use collective data to identify trends for diversity, equity, and inclusion purposes and to inform decision making with a view to promoting or maintaining diversity, equity, and inclusion, with your explicit written consent.
2) Where we need to carry out our legal obligations or exercise rights in the field of employment law.
3) Where it is needed in the public interest, such as equal opportunities monitoring.
4) For the provision of Occupational Health services.

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 vital interests (or someone else's vital interests) and you are not capable of giving your consent,or where you have already made the information public.

Situations in which we will use your sensitive personal information.

We may use your special category personal information in the following ways:

- The organisation processes health information if it needs to make reasonable adjustments to the recruitment process for candidates who have a disability. This is to conduct its obligations and exercise specific rights in relation to employment.
- Where the organisation processes 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.
- For some roles, the organisation is obliged to seek information about criminal convictions and offences. Where the organisation seeks this information, it does so because it is necessary for it to conduct its obligations and exercise specific rights in relation to employment.
- The organisation may use special category information that you provide, such as information about ethnic origin, sexual orientation, health or religion or belief, on a collective basis and through trend identification to make decisions around Diversity, Equity and Inclusion with a view to continually improving its recruitment processes and ensuring that they remain fair and robust.

Do we need your consent?

In most cases, we do not need your consent to use your personal information, including for most of the special categories of personal information described above. In limited circumstances, we may ask for your consent to allow us to process certain personal information, particularly sensitive data. If we do so, we will provide you with full 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.

Right to withdraw consent.

In the limited circumstances where you may have provided your consent to the collection, processing, and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact Simon Mahaffey at the address given above. 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.

Data Sharing.

Your information will be shared internally for the purposes of the recruitment exercise and may also be shared with our group companies for this reason. This includes members of the HR and recruitment team, interviewers involved in the recruitment process, managers in the business area with a vacancy and IT staff if access to the data is necessary for the performance of their roles.

The organisation will not otherwise share your data with third parties unless your application for employment is successful and it makes you an offer of employment. The organisation will then share relevant personal data with former employers to obtain references for you, employment background check providers to obtain necessary background checks and the Disclosure and Barring Service to obtain necessary criminal records checks.

Where we share your data with our service providers, we require our service providers to enter contracts with us which oblige them to respect the security of your personal information and to treat it in accordance with the law. You can therefore expect a similar degree of protection in respect of your personal information.

The following activities may be carried out by third-party service providers: payroll, IT providers and recruitment services, pre-engagement screening service provider.

We may also share your personal information with third parties where required by law, where it is necessary to administer the working relationship with you or where we have a legitimate interest in doing so. Examples include HMRC, central and local government, professional and regulatory bodies, educational organisations, background checks and identity verification, banks, lenders, landlords, courts, and tribunals.

Transferring information outside the UK.

Some of the service providers we use may be in other countries. As a result, your information may be processed outside the UK and European Economic Area (EEA). In all cases we will make sure that your information is adequately protected. Whenever we transfer your personal data out of the UK, we ensure a similar degree of protection is afforded to it by ensuring adequate safeguards are implemented, which may include:

- The transfer of personal information is to a country that has been deemed to provide an adequate level of protection for personal data under UK adequacy regulations.
- We will put in place contracts with service providers which incorporate the standard contractual clauses for data processors recognised or issued in accordance with UK data protection law or other contracts which provide equivalent protection.

Please contact us, if you want further information on the specific mechanism used by us when transferring yourpersonal data outside of the UK or EEA.

Data Security.

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 employees, agents, contractors and other third parties who have a business need to know. They process your personal information on our instructions, and they are subject to a duty of confidentiality.

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

Third parties will only process your personal information on our instructions and where they have entered a contract requiring them to treat the information confidentially and to keep it secure.

Should you require any further details please contact IQUW's Data Protection Officer, dpo@iquw.com

Data Retention.

We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including fr the purposes of satisfying any legal and accounting requirements. To determine the appropriate retention period forpersonal data, we consider the amount, nature and sensitivity of the personal data, any statutory retention requirements that apply, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and any other archiving or historical record-keeping obligations.

Where possible we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information indefinitely without further notice to you. Any information which is no longer needed will be destroyed securely.

As above, if your application for employment is unsuccessful, the organisation will hold your data on file for 12 months after the end of the relevant recruitment process. If you agree to allow the organisation to keep your personal data on file, the organisations will hold your data for 12 months for consideration for future employment opportunities. At the end of the second period or once you withdraw your consent, your data is deleted.

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

Your rights of access, correction, erasure, and restriction

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 the recruitment process, or if you discover any errors or omissions.

Subject to the provisions of the Data Protection Act, you may have the following rights:

- 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.
- 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 personalinformation where there is no lawful reason for us to continue to process it.
- Object to processing of your personal information where we are relying on a legitimate interest (or those of athird party) and you have a particular justification for objecting to processing on this ground.
- 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 legalbasis for processing it.
- Request the transfer of your personal information to another party.

If you want to exercise any of your rights, please contact HRCentral@iquw.com by email or in writing at the address above.

We may need to request specific information from you to help us confirm your identity and your right to access the information (or to exercise any of your other rights). This is an appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it. If you are not satisfied with our use of your personal data or our response to any request by you to exercise your rights in relation to your personal data, please contact DPO@iquw.com (Simon Mahaffey) at the address given above.

What if you do not provide personal data?

You are under no obligation to provide data to the organisation during the recruitment process. However, if you do not provide the personal data required, the organisation will not be able to process your application.

You are under no obligation to provide information for equal opportunities monitoring purposes and there are no consequences for your application if you choose not to provide such information.

Automated decision-making

Recruitment processes are not based solely on automated decision-making.

Complaints to the ICO

You also have a right to make a complaint to the Information Commissioner:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
Tel: 0303 123 1113 (local rate)
Email: icocasework@ico.org.uk

Version History

Version #	Updates	Name	Date
1.0	Document created	Training & Development	16/05/21
2.0	Page guidance updated	Training & Development	16/06/21
2.1	Updated reference to email and sensitive data	DPO	31/05/22
3.0	DPO/Legal updates	Legal amendments to template and criminal information as well as	31/05/2022
4.0	Final version	Legal approved/DPO approved	29/06/22 and 30/06/22
5.0	Final Version – London Address Change	DP Analyst	13/09/22
5.1	Grammatical changes – General review	DP Analyst	09/08/23
5.2	Further grammatical changes	DP Analyst	10/08/23
5.3	Grammar changes and format/structure changes	DPO	10/08/23
5.4	Update to include decision making around DE+I information	DP Analyst	22/03/24
5.5	Review by Legal dept. for check. Amendments made.	Sam Gernon	15/04/24
6.0	Final Version	DP Analyst	17/04/24
6.1	Change of DPO	DP Analyst	14/05/24