Job Applicant Privacy Notice

Data controller: Ipeco Holdings Ltd, Aviation Way, Southend-on-Sea, Essex, SS2 6UN

As part of any recruitment process, the organisation collects and processes personal data relating to job applicants. The organisation is committed to being transparent about how it collects and uses that data and to meeting its data protection obligations.

What information does the organisation collect?

The organisation collects a range of information about you. This includes:

- your name, address and contact details, including email address and telephone number;
- details of your qualifications, skills, experience and employment history;
- information about your current level of remuneration, including benefit entitlements;
- whether or not you have a disability for which the organisation needs to make reasonable adjustments during the recruitment process;
- information about your entitlement to work in the UK;
- details of whether you have been convicted of a criminal offence including date(s) and sentence(s) passed which are not spent;
- information about your criminal record via the Disclosure and Barring Service (where necessary for the role);
- information about your driving record (where necessary for the role); and
- equal opportunities monitoring information, including information about your ethnic origin, sexual orientation, health, and religion or belief.

The organisation collects this information in a variety of ways. For example, data might be contained in application forms or CVs, obtained from your passport, driving licence or other identity documents, or collected through interviews or other forms of assessment, including practical and written tests.

The organisation will also collect personal data about you from third parties, such as references supplied by former employers and information from criminal records checks where necessary for the role. The organisation will seek information from third parties only once a job offer to you has been made and will inform you that it is doing so.

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 does the organisation process personal data?

The organisation needs to process data to take steps at your request prior to entering into a contract with you. It also needs to process your data to enter into a contract with you.

In some cases, the organisation needs to process data to ensure that it is complying with its legal obligations. For example, it is required to check a successful applicant's eligibility to work in the UK before employment starts.

The organisation has a legitimate interest in processing personal data during the recruitment process and for keeping records of the process. Processing data from job applicants allows the organisation to manage the recruitment process, assess and confirm a candidate's suitability for employment and decide to whom to offer a job. The organisation may also need to process data from job applicants to respond to and defend against legal claims.

Where the organisation relies on legitimate interests as a reason for processing data, it has considered whether or not those interests are overridden by the rights and freedoms of employees or workers and has concluded that they are not.

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 carry out 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, religion or belief, age, gender or marital status, this is done for the purposes of equal opportunities monitoring.

The organisation processes details of unspent convictions in order to assess a candidate's suitability for employment. An unspent conviction will not, in itself, debar a person from being appointed to a post and suitable applicants will not be refused posts because of offences which are not relevant to, and do not place them at or make them a risk in the role for which they are applying. All cases will be examined on an individual basis and will take into account whether the conviction is relevant to the position, the seriousness of the offence and how recent it was, and whether it was a one-off or one of a number. The organisation recognises the contribution that ex-offenders can make as employees and welcome applications from them.

For some roles, the organisation is obliged to seek information about criminal convictions and offences from the Disclosure and Barring Service. Where the organisation seeks this information, it does so because it is necessary for it to carry out its obligations and exercise specific rights in relation to employment.

The organisation processes details of your driving record, obtained from your driving licence and the Government Licence Check Service, where it is a requirement of the role for the candidate to hold a clean driving record.

Who has access to data?

Your information will be shared internally for the purposes of the recruitment exercise. This includes members of the HR 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. Your information is also accessible by the Chief Executive Officer and the Finance Director (Head of HR, Finance, Training Centre, and Property), if access to the data is necessary for the performance of their roles.

The organisation will not 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 your data with former employers to obtain references for you and the Disclosure and Barring Service to obtain necessary criminal records checks where applicable to the role.

The organisation will not transfer your data outside the European Economic Area.

How does the organisation protect data?

The organisation takes the security of your data seriously. It has internal policies and controls in place to ensure that your data is not lost, accidentally destroyed, misused or disclosed, and is not accessed except by our employees in the proper performance of their duties. For more information on data security, please refer to the Information Security Policy, the Backup Policy and the Data Protection Policy, a copy of which can be obtained by request from Recruitment@Ipeco.com.

For how long does the organisation keep data?

If your application for employment is unsuccessful, the organisation will hold your data on file for 6 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 on file for a further 6 months for consideration for future employment opportunities. At the end of that period or once you withdraw your consent, your data is deleted or destroyed.

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 the Employee Privacy Notice.

Whilst primary instances of data in systems will be erased in accordance with our Data Retention Schedule, the organisation may store personal data in backup archives for longer than the specified periods detailed in the Schedule. This is because it is impractical to isolate individual personal data within the archive. Retention rules have been put in place so that personal data in backup archives is retained for as short a time as necessary before being automatically deleted. More information concerning backup archives and data retention timeframes can be found in the Information Security Policy, the Backup Policy and the Data Retention Schedule, copies of which can be requested from Recruitment@Ipeco.com.

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 the organisation to change incorrect or incomplete data;
- require the organisation 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 the organisation is relying on its legitimate interests as the legal ground for processing; and
- ask the organisation to stop processing data for a period if data is inaccurate or there is a dispute about whether or not your interests override the organisation's legitimate grounds for processing data.

If you would like to exercise any of these rights, please contact Recruitment@Ipeco.com.

If you believe that the organisation has not complied with your data protection rights, you can complain to the Information Commissioner.

What if you do not provide personal data?

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

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.