



## **idverde Candidate Privacy Policy**

### **1. What is the purpose of this document?**

idverde UK Limited is the "controller" of your personal data. This means we decide how your personal information is collected, used and stored. We are giving you this privacy notice because you are applying for work with us, whether as an employee, worker or contractor. It explains what personal data we use during the recruitment process, why we use it, and how long we usually keep it. It also gives you the information we must provide under the UK General Data Protection Regulation (UK GDPR).

### **2. Data protection principles**

We will comply with data protection law and principles, which means that your data will be:

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

### **3. Who is your personal information collected from?**

We collect personal information about candidates from the following sources:

- You, the candidate;
- Recruitment agencies;
- Companies that carry out employment screening and checks for us;
- Publicly accessible sources, where permissible.

### **4. The kind of information we hold about you**

As part of your application, we will collect, store and use the following categories of personal information about you:

- Information you provide in your application form or CV, including your name, address, telephone number, personal email address, education, qualifications and employment history.
- Any information you provide to us during the interview process.
- Information we receive from other sources mentioned in this notice.

Where needed and where the law allows, we may also collect, store and use the following types of more sensitive personal information:

- Information about your race or ethnicity, religion or beliefs
- Information about your health, including any medical condition.
- Information about criminal convictions and offences.

## **5. How we will use information about you**

We will use the personal information we collect about you to:

- Assess your skills, qualifications, and suitability for the role.
- Carry out background and reference checks, where applicable.
- Communicate with you about the recruitment process.
- Keep records related to our hiring processes.
- Comply with legal or regulatory requirements.

We may use your personal information:

- To take steps before entering into an employment contract with you;
- To decide whether to enter into an employment contract with you, where this is in our legitimate interests; and
- To comply with the law.

## **6. If you fail to provide personal information**

If you do not provide information we ask for and need to assess your application, such as evidence of your qualifications or work history, we may not be able to process your application. For example, if the role requires references or a credit check and you do not provide the relevant details, we may not be able to take your application further.

## **7. How we use particularly sensitive personal information**

Where appropriate, we will use your more sensitive personal information in the following ways:

- We use information about disability to consider whether we need to provide appropriate adjustments during the recruitment process, for example whether adjustments need to be made during interview.
- We use information about racial or ethnic origin, religious or philosophical beliefs, disability or sexual orientation for equal opportunities monitoring and reporting.

## **8. Information about criminal convictions**

We may process information about criminal convictions where this is needed for the role.

Some of our clients require us to carry out a criminal records check. Where this applies, and where required, we will ask for your consent to collect information about your criminal convictions history so we can assess whether you are suitable for the role.

## **9. Automated decision-making**

We do not make decisions that will have a significant impact on you based solely on automated decision-making.

## **10. Data sharing**

### **Why might you share my personal information with third parties?**

We share your personal data with third parties who need it to process your application, such as our recruitment agency partners and providers who carry out pre-employment screening for us. We also share your personal data with the relevant teams within idverde and its group companies where they need it to assess or process your application.

## **11. Cross-border data transfers**



If we transfer your personal information to the European Economic Area (EEA), for example to other members of the *idverde* group, we will do so in line with the UK government's adequacy decision for EEA countries.

## **12. 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 will only 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 any applicable regulator of a suspected breach where we are legally required to do so.

## **13. Data retention**

### **How long will you use my information for?**

We keep your personal information for 12 months after we tell you our decision about whether to appoint you to the role. We keep it for this period so that, if there is a legal claim, we can show that we did not discriminate against candidates on prohibited grounds and that we ran the recruitment process fairly and transparently. After this period, we will securely delete or destroy your personal information in line with applicable laws and regulations.

If you are successfully recruited, your personal information will be retained in accordance with our employee privacy policy.

## **14. Rights of access, rectification, erasure, objection, restriction and data portability**

### **Your rights in connection with personal information**

In some circumstances, the law gives you the right to:

- **Request access** to your personal information (commonly known as making 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 rectification** 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 have the 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.
- **Withdraw** your consent at any time for processing based on consent.

If you would like to exercise any of these rights, please contact [compliance@idverde.co.uk](mailto:compliance@idverde.co.uk).

### **15. Third party sites**

The careers page on our website includes links to third-party websites managed by our recruitment partners. We do not control these websites. They have their own privacy notices explaining how they collect, share and use your data.

### **16. Complaints**

You have the right to complain to the Information Commissioner's Office (ICO), the UK regulator for data protection issues, for example if you think we have not responded properly to a request about your personal information or are holding inaccurate information about you. Before contacting the ICO, please raise your concern with us first or ask us for clarification if anything is unclear. The ICO will usually expect you to do this before it reviews your complaint.

Any complaint can be raised either via email to [compliance@idverde.co.uk](mailto:compliance@idverde.co.uk) or by post to Data Protection, Octavia House, Westwood Way, Westwood Business Park, Coventry CV4 8JP.

To help us deal with your complaint as quickly as possible, please provide full details of your concern and copies of any key documents.

We must acknowledge your complaint within 30 days, but we aim to acknowledge it within 7 working days of receiving it. We also aim to:

- Ask for any further information we need for clarification or identification within 10 working days of acknowledging your complaint;
- Give you updates at least every 30 days after we acknowledge your complaint; and
- Reach an outcome within 60 days of acknowledging your complaint.

If your complaint is complex, serious or covers several issues, it may take us longer to investigate and resolve. If that happens, we will keep you informed about the likely timescales.

Once we have completed our investigation, we will tell you the outcome and explain our findings, whether we have upheld your complaint in whole or in part, and any action taken or proposed. If we do not propose any action, we will explain why.

If you are not satisfied with the outcome or the way your complaint was handled, you can ask for it to be reviewed by another member of our leadership team. They will review the matter and respond, either confirming the original decision or making a new one. They will aim to respond within 60 working days of the referral.

If you still remain dissatisfied after that, you can complain to the ICO or seek a remedy through the courts.

Last updated June 2026