



Candidate Privacy Notice.



Version	Revision Date	Revised By	Classification	Changes
0.1	01/12/2021	Compliance (KQ)	Public	Initial Release
1.0	17/01/2022	Compliance (KQ)	Public	Signed off version
2.0	27/04/2023	Compliance (KQ)	Public	changed data retention period and small formatting issues
3.0	12/01/2024	Compliance (KQ)	Public	Reviewed
4.0	25/10/2024	Compliance (KQ)	Public	reviewed - retention period amended + recordings and transcripts addendum
5.0	08/09/2026	Compliance (AI)	Public	Redrafted for Ashby ATS (US hosting, AI tools), Data (Use and Access) Act 2025 changes,, 12-month retention and complaints procedure

Contents

What is the purpose of this document?	2
Data protection principles	2
The kind of information we hold about you	2
How is your personal information collected?	3
How we will use information about you	4
If you fail to provide personal information	5
How we use particularly sensitive personal information	6
Information about criminal convictions	6
Automated decision-making and use of AI	6
Data sharing	7
1. Why might you share my personal information with third parties?	7
2. International transfers	7
3. Data security	8
4. Data retention	8
4.1 How long will you use my information for?	8
4.2 Rights of access, correction, erasure, and restriction	9
Contact us and complaints	10
Addendum: interview recordings, transcripts and AI-generated summaries	11

What is the purpose of this document?

Plentific Ltd (company number **08275972**, registered office **Third Floor Yarnwicke, 119-121 Cannon Street, London, England, EC4N 5AT**) ("Plentific", "we", "us") is the "controller" of the personal data described in this notice. This means that we are responsible for deciding how we hold and use personal information about you.

This notice applies to you if you apply for a role with us (whether as an employee, worker or contractor), if you are referred to us, or if we identify and contact you about a role. It explains how and why we use your personal data during the recruitment process, how long we keep it, who we share it with and what your rights are. It provides the information we must give you under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (together, "Data Protection Law").

We use Ashby, a recruitment platform provided by Ashby, Inc., to manage our recruitment. When you apply through our careers site or a job board, or when we contact you about a role, your information is held in Ashby. Please see "Data sharing" and "International transfers" below for more about this.

If your application is successful, the personal data we collected during recruitment will become part of your personnel file and will be handled in accordance with our Employee Privacy Notice, which we will give you when you join.

We may update this notice from time to time. The current version and date are shown at the top of this document.

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.

The kind of information we hold about you

In connection with your application for work with us, we will collect, store, and use the following categories of personal information about you:

- **Identity and contact details:** your name, title, address, telephone number and personal email address, and links to any professional profiles (for example LinkedIn) you provide.
- **Application information:** the information in your CV, covering letter and application form, including your employment history, qualifications, skills, notice period and salary expectations.
- **Information from recruitment agencies:** where an agency introduces you, your CV, notice period and salary expectations.
- **Interview and assessment information:** notes, scores and feedback from interviews, and the results of any tests or assessments you complete.
- **Interview recordings, transcripts and AI-generated summaries,** which we may use unless you tell us you prefer not to be recorded (see the Addendum at the end of this notice).
- **Right to work information:** your nationality, immigration status and copies of identity documents such as your passport or visa, together with your date of birth, collected at the offer stage.
- **Health information:** information about any disability or health condition you tell us about so that we can make reasonable adjustments.
- **Equality and diversity monitoring information,** if you choose to provide it (see "How we use particularly sensitive personal information").
- **Technical information** generated when you use our careers site or communicate with us through Ashby, such as your IP address, device and browser type, the source of your application, and whether you open or click on emails we send you.

How is your personal information collected?

We collect personal information about candidates from the following sources:

- You, when you apply, complete a form, attend an interview or assessment, or correspond with us.
- Recruitment agencies and search firms acting on our behalf or on yours.
- Job boards and professional networking sites (for example LinkedIn), where you have made your profile available to recruiters or applied through them.
- Our employees, where they refer you for a role.
- Previous applications you have made to us, which are held in Ashby.
- Your referees, once you have given us their details and authorised us to contact them.
- Background-check providers – a credit reference agency, and the Disclosure and Barring Service (DBS) or a registered umbrella body – where checks apply to the role.
- Publicly available sources, where we need to verify information you have given us.

If we obtain your details from a source other than you - for example, if a recruiter finds your profile on LinkedIn or an employee refers you - we will give you this notice (or a link to it) when we first contact you, and in any event within one month of obtaining your details.

How we will use information about you

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

- Assess your skills, qualifications, experience and suitability for the role, including shortlisting applications (see "Automated decision-making and use of AI").
- Communicate with you about your application and the recruitment process, including by email, telephone and text message, and schedule interviews.
- Carry out reference, right to work, credit and criminal record checks, where these apply to the role.
- Make reasonable adjustments to the recruitment process where you need them.
- Keep records of our recruitment activity and produce aggregate reports so that we can understand and improve how we recruit (for example, time to hire and the sources of applications).
- Detect and prevent fraudulent or duplicate applications.
- Keep your details on file and contact you about future roles that may interest you, unless you ask us not to.
- Comply with our legal and regulatory obligations and establish, exercise or defend legal claims.

Data protection law requires us to have a lawful basis for each use of your personal data. The bases we rely on are set out below.

Purpose	Lawful basis
Assessing your application and deciding whether to offer you a role	Taking steps at your request before entering into a contract with you (Article 6(1)(b)); and our legitimate interest in recruiting suitable people for our business (Article 6(1)(f)).
Communicating with you and scheduling interviews	Steps before entering into a contract (Article 6(1)(b)); legitimate interests (Article 6(1)(f)).
Right to work checks	Compliance with our legal obligations under the Immigration, Asylum and Nationality Act 2006 (Article 6(1)(c)).
Reference checks	Our legitimate interest in verifying the information you have given us (Article 6(1)(f)).
Credit checks (for e.g. roles with power of attorney responsibilities only)	Our legitimate interest in protecting our business and our clients where a role involves financial responsibility (Article 6(1)(f)) and/or power of attorney obligations. We will tell you before we carry out a credit check.
Criminal record checks (for eligible roles only)	Our legitimate interests in protecting our clients, their residents and our systems (Article 6(1)(f)) and, where the role is one for which a check is required by law, compliance with that legal obligation (Article 6(1)(c)).

Reasonable adjustments and equality monitoring	Compliance with our legal obligations under the Equality Act 2010 (Article 6(1)(c)). See "How we use particularly sensitive personal information" for the additional conditions we rely on.
Recruitment records, reporting and process improvement; fraud prevention	Our legitimate interests in running an efficient, fair and secure recruitment process (Article 6(1)(f)).
Contacting you about future roles	Within 12 months of your application: our legitimate interest in filling roles from people who have already shown an interest in working for us (Article 6(1)(f)) – you may opt out at any time. Beyond 12 months: your consent (Article 6(1)(a)), which you may withdraw at any time.
Interview recordings, transcripts and AI-generated summaries	Your consent (Article 6(1)(a)) – see the Addendum.
Complying with legal obligations and defending legal claims	Compliance with legal obligations (Article 6(1)(c)); our legitimate interest in protecting our legal position (Article 6(1)(f)).

Where we rely on legitimate interests, we have considered and balanced them against your interests and rights, and we do not consider that our processing overrides them. You can ask us for more information about this assessment.

Having received your application, we will first review it to decide whether you meet the basic requirements for the role. For roles that attract a high volume of applications we may use an AI-assisted review tool within Ashby to help with this initial review (see "Automated decision-making and use of AI"); a member of our recruitment team always reviews the outcome and makes the decision. If you are shortlisted, we will invite you to one or more interviews or assessments and use the information you provide to decide whether to offer you the role. If we offer you the role, the offer will be conditional on satisfactory references and right to work checks and, where they apply to the role, credit and criminal record checks.

If you fail to provide personal information

If you do not provide information that we need to consider your application – for example, evidence of your qualifications, work history or right to work, or the details we need to carry out a reference, credit or criminal record check that applies to the role – we may not be able to take your application further. We will tell you if this is the case. Where something is optional - for example, the recording of an interview or equality monitoring - declining will not affect your application.

How we use particularly sensitive personal information

"Special category" personal data - such as information about your health, racial or ethnic origin, religion, sexual orientation or trade union membership - needs a higher level of protection. We will use it only in the following ways, and only where we have both a lawful basis (see above) and one of the additional conditions in Article 9 of the UK GDPR and Schedule 1 to the Data Protection Act 2018:

- **Health and disability.** We will use information about a disability or health condition that you tell us about to consider whether we need to make reasonable adjustments during the recruitment process, for example to a test or interview. We do this to comply with our obligations under the Equality Act 2010 (Article 9(2)(b); Schedule 1, Part 1, paragraph 1).
- **Equality and diversity monitoring.** We may invite you to complete a voluntary equal opportunities survey. Your answers are collected through a separate survey tool in Ashby, are held separately from your application, are not visible to the people deciding on your application, and are used only in anonymised, aggregate form to monitor and promote equality of opportunity (Article 9(2)(g); Schedule 1, Part 2, paragraph 8). You may decline to answer, or select "prefer not to say", for any question.
- **Right to work.** The documents you provide to prove your right to work may reveal your nationality or ethnic origin. We use them only to comply with our legal obligation to check your right to work (Article 9(2)(b); Schedule 1, Part 1, paragraph 1).
- **Legal claims.** We may use special category data where necessary to establish, exercise or defend legal claims (Article 9(2)(f)).

Information about criminal convictions

We do not process information about criminal convictions.

Automated decision-making and use of AI

We use some artificial intelligence (AI) tools within Ashby to help our recruitment team work efficiently. We do not make any decision about your application that has a legal or similarly significant effect on you based solely on automated processing; a member of our team always reviews the information and makes the decision. The tools we use are:

- **AI-assisted application review.** For roles with a high volume of applications, Ashby can compare the information in your application against requirements for the role that our recruitment team has defined (for example, essential skills or experience) and highlight applications that appear to match. It does not rank you against other candidates or reject applications automatically. A recruiter reviews the results and decides who is shortlisted.
- **AI Notetaker.** With your consent, Ashby's notetaker can join a video interview to record, transcribe and summarise the conversation, so that interviewers can focus on you rather than on taking notes. See the Addendum at the end of this notice.

- **AI candidate assistant.** Our recruitment team can ask Ashby questions about the information already held in your candidate record (for example, "summarise this candidate's experience of X") to help them prepare for interviews and write up feedback. It works only on information we already hold about you and does not gather new information.

AI-generated outputs can contain errors. Our team is trained to treat them as an aid and to check them against the source information before relying on them. We have assessed the data protection risks of these tools and keep them under review. Ashby does not use your personal data to train its AI models.

If we ever propose to make a decision about you based solely on automated processing, we will tell you in advance, explain how the decision is made, and give you the right to ask for a human to reconsider it, to make representations and to contest the decision, as data protection law requires. You can ask us at any time how AI has been used in connection with your application by contacting us using the details below.

Data sharing

1. Why might you share my personal information with third parties?

We share your personal information with the following categories of recipient, only where this is necessary for the purposes described in this notice:

- **Our recruitment platform provider, Ashby, Inc.,** which hosts our applicant tracking system, careers site, interview scheduling and AI tools and acts as our processor.
- **Other service providers** that support our recruitment process, such as video-conferencing and calendar providers used for interviews, e-signature tools for offer letters, and online assessment providers where a role requires them.
- **Recruitment agencies and search firms,** where you were introduced to us by one or we use one to manage a vacancy.
- **Referees you have nominated,** and your current or former employers or educational institutions, to verify the information you have given us.
- **Other companies in the Plentific group** (Plentific GmbH), where roles are shared across the group or where group HR, IT or legal functions support our recruitment.
- **Our professional advisers** (such as lawyers, auditors and insurers), and regulators, courts or law enforcement agencies where we are required to disclose information by law or to protect our legal rights.
- **If you are hired, our HR and payroll systems and providers,** so that we can set you up as an employee.

Our service providers act as our processors. They are contractually required to keep your information secure, to use it only on our instructions and for the purposes we specify, and not to use it for their own purposes.

2. International transfers

Ashby stores and processes data in the United States. Some of our other providers, and companies in our group, may also be located outside the United Kingdom. Whenever we transfer your personal data outside the UK we make sure that it is protected to a standard equivalent to UK data protection law by relying on one of the following safeguards:

- the recipient's certification under the UK Extension to the EU-US Data Privacy Framework (this applies to Ashby);
- the UK International Data Transfer Agreement, or the UK Addendum to the EU Standard Contractual Clauses, together with any additional measures identified in our transfer risk assessment; or
- for transfers to the European Economic Area, the UK's adequacy regulations.

You can ask us for more information about these safeguards, or for a copy of the relevant documents, using the contact details below.

3. 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.

4. Data retention

4.1 How long will you use my information for?

How long we keep your information depends on the outcome of your application and how you have asked us to use it:

- **Unsuccessful applications.** We keep your personal information for 12 months after we tell you our decision. We keep it for this period so that we can respond to any queries or complaints about the process and show, if a claim is made, that we have conducted the recruitment exercise fairly and without discrimination.
- **Future roles (talent pool).** During those 12 months we may contact you about other roles that may suit you; you can ask us not to at any time. Before the 12 months end, we will ask whether you would like us to keep your details for a further 12 months so that we can continue to contact you. If you agree, we will ask you again at the end of that period; if you decline or do not respond, we will delete or anonymise your details.
- **Interview recordings and transcripts.** These are deleted six months after we tell you the outcome of your application. AI-generated summaries and interviewer feedback are kept with your candidate record for the periods above (see the Addendum).
- **Pre-employment check information.** Criminal record certificate information is destroyed within six months of the recruitment decision. Credit check results are

kept only for as long as needed to make the decision and are then deleted or, if you are hired, transferred to your personnel file.

- **Successful applications.** Your recruitment information is transferred to your personnel file. Our Employee Privacy Notice explains how long we keep it.
- **Anonymised information.** We may keep anonymised statistical information about our recruitment indefinitely. This cannot be used to identify you.

These retention periods are applied automatically within Ashby. At the end of the relevant period we will securely delete or anonymise your personal information, unless we are required to keep it for longer to comply with a legal obligation or in connection with a legal claim.

4.2 Rights of access, correction, erasure, and restriction

Your rights in connection with personal information

Under certain circumstances, by law you have 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 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 where we rely on your consent (for example, for interview recordings or for staying in our talent pool). Withdrawing consent does not affect the lawfulness of anything we did before you withdrew it, and will not affect your application.
- **Not be subject to a decision based solely on automated processing** that has legal or similarly significant effects on you and, where such a decision is made, to obtain human intervention, express your point of view and contest the decision.

To exercise any of these rights, please contact us using the details below. We will normally respond within one month. Where a request is complex, or you have made several requests, we may extend this by up to two further months; we will tell you if this is the case. We may need to ask you for information to confirm your identity or to clarify what you are asking for, and the time we have to respond will not start until we have received it.

We will not charge you for exercising your rights unless your request is manifestly unfounded or excessive.

Contact us and complaints

If you have any questions about this privacy notice or how we handle your personal information, or you wish to exercise any of your rights, please contact our privacy team at Privacy@plentific.com.

If you are unhappy with the way we have handled your personal information, you have the right to complain to us. Please contact us using the details above: we will acknowledge your complaint within 30 days and let you know the outcome without undue delay. You also have the right to complain at any time to the Information Commissioner's Office (ICO), the UK's data protection regulator (ico.org.uk), although we would welcome the chance to address your concerns first.

Addendum: interview recordings, transcripts and AI-generated summaries

We use Ashby's AI Notetaker for some interviews. It is in our legitimate interest in ensuring accurate, fair and consistent assessment of your interview without interviewer note-taking bias. You have the right to object to the recording at any time, including when we first notify you or at the start of the interview (including during the interview), the interview will go ahead without recording and this will have no effect on your application.

- **Purpose.** Recordings, transcripts and summaries are used only to help interviewers assess your interview accurately and consistently, to write up their feedback, and to allow members of the hiring team who could not attend to review the interview. They are not used for any other purpose and are not used to train AI models.
- **Accuracy.** Transcripts and AI-generated summaries can contain mistakes. Interviewers are required to check them against the recording or their own recollection before relying on them, and decisions about your application are always made by people. You can ask for a copy of your transcript and for corrections to be made.
- **Who processes them.** Recordings, transcripts and summaries are stored in Ashby (see "Data sharing" and "International transfers" for where Ashby stores data and the safeguards that apply). The video-conferencing platform used for the interview also processes the call.
- **Storage and access.** Recordings and transcripts are stored securely and are accessible only to the interviewers, the hiring manager and the recruitment team for the role.
- **Retention.** Recordings and full transcripts are deleted six months after we tell you the outcome of your application. AI-generated summaries and interviewer feedback are kept with your candidate record for the retention periods set out in this notice.
- **Your rights.** You may withdraw your consent at any time, ask for access to your recording, transcript and summary, ask us to correct inaccuracies, or ask us to delete them, by contacting us using the details in this notice.