



## Privacy Notice for job applicants in the EU

# Table of Contents

1.	What is the purpose of this document?.....	3
2.	Data protection principles .....	3
3.	The kind of information we hold about you .....	3
4.	How is your personal information collected? .....	4
5.	How we will use information about you.....	4
6.	If you fail to provide personal information.....	5
7.	How we use particularly sensitive personal information .....	5
8.	Information about criminal convictions.....	5
9.	Automated decision-making.....	5
10.	Data sharing .....	6
10.1.	Why might you share my personal information with third parties? .....	6
10.2.	Transferring information outside the EU .....	6
11.	Data security .....	7
12.	Data retention.....	7
13.	Rights of access, correction, erasure, and restriction .....	8
14.	Right to withdraw consent.....	8
15.	Data protection officer .....	9
16.	Changes to this privacy notice.....	9

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

The Aptus Health Group, its affiliates and subsidiaries including Aptus Health International UK Pvt Ltd and Aptus Health International France SAS in the European Union (“Aptus Health”) are committed to protecting the privacy and security of your personal information.

You are applying for work with us (whether as an employee, worker or contractor) and this privacy notice is intended to make you aware of how and why your personal data will be used, namely for the purposes of the recruitment exercise, and how long it will usually be retained for. It provides you with certain information that must be provided under the General Data Protection Regulation ((EU) 2016/679) (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. 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:

- The information you have provided to us in your curriculum vitae and covering letter.
- The information you have provided on our application form, including name, title, address, telephone number, personal email address, date of birth, gender, employment history, qualifications.
- Any information you provide to us during an interview.
- References and background.
- Any tests results, as applicable.
- Salary expectations.

## 4. How is your personal information collected?

We collect personal information about candidates from the following sources:

- You, the candidate.
- Recruitment agencies such as AMETIX, Allegis (Teksystems, Aston Carter), InTeam, Computer Futures, Stanton Wallace, Mobiskill, Rhezo, Urban Linker, Cos2biz, Agence E, Fed Human, Michael Page Healthcare, Tungsten Noble, Barrington James and Robert Walters, from which we collect the following categories of data: information that you submit to such agencies including CV, salary expectations, references, brief of interview, potentially personality test results.
- Your named referees, from whom we collect the following categories of data: information about your prior experiences, feedback about your collaboration and performance.

## 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 you apply for.
- 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.

It is in our legitimate interests to decide whether to appoint you to a role since it would be beneficial to our business to appoint someone to that role.

We also need to process your personal information to decide whether to enter into a contract of employment with you.

Having received your CV, covering letter and/or your application form and, as and if applicable to the role you apply for, results from test, we will then process that information to decide whether you meet the basic requirements to be shortlisted for the role. If you do, we will decide whether your application is strong enough to invite you for an interview. If we decide to call you for an interview, we will use the information you provide to us at the interview to decide whether to offer you the role. If we decide to offer you the role, we will then take up references and potentially carry out a criminal record check before confirming your appointment.

## 6. If you fail to provide personal information

If you fail to provide information when requested, which is necessary for us to consider your application (such as evidence of qualifications or work history), we will not be able to process your application successfully. For example, if we require references for this role and you fail to provide us with relevant details, we will not be able to take your application further.

## 7. How we use particularly sensitive personal information

We may use your particularly sensitive personal information in the following ways, subject to applicable laws:

- If and as applicable, we will use information about your disability status to consider whether we need to provide appropriate adjustments during the recruitment process, for example whether adjustments need to be made during a test or interview.

## 8. Information about criminal convictions

We envisage that, depending on the position you apply for and always subject to applicable laws and regulations, we may process information about criminal convictions. Should we do so, you will be provided with detailed information and such criminal record check would be carried out in order to satisfy ourselves that there is nothing in your criminal convictions history which makes you unsuitable for the role.

We will have in place appropriate safeguards which we are required by law to maintain when processing such data.

## 9. Automated decision-making

You will not be subject to decisions that will have a significant impact on you based solely on automated decision-making.

## 10. Data sharing

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

We will only share your personal information with the following third parties for the purposes of processing your application: other affiliates of the Aptus Health Group, your former employees for references checks, recruitment agencies such as AMETIX, Allegis (Teksystems, Aston Carter), InTeam, Computer Futures, Stanton Wallace, Mobiskill, Rhezo, Urban Linker, Cos2biz, Agence E, Fed Human, Michael Page Healthcare, Tungsten Noble, Barrington James and Robert Walters, our application management system such as Newton. We screen our third-party service providers in order to ensure that they provide an “adequate” level of protection of your personal data. All our third-party service providers and other entities in the group are required to take appropriate security measures to protect your personal information in line with our policies. We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

### 10.2. Transferring information outside the EU

When we transfer personal information we collect about you, to third parties providers or to Aptus Health affiliates, we ensure that such transfers are made either to countries that the EU Commission has deemed “adequate”, or that additional safeguards are in place in order to protect your personal information.

Within Aptus Health, transfers of personal information may be made to the Aptus Health affiliates in the United States of America or in India, as part of our recruitment process, for instance in order to review your application, to set up or conduct interviews. Such transfers are made on the basis of Standard Data Protection Contractual Clauses adopted by the European Union Commission. This means that the legal entity to which we transfer your data is bound by a contractual obligation to provide an adequate level of protection for your personal information. Aptus Health legal entities in the United States of America provide additional guarantee of protection to your personal data through a Privacy Shield certification. To review Aptus Health's representation on the Privacy Shield list, see the US Department of Commerce's Privacy Shield self-certification list located at: <https://www.privacyshield.gov/list>. To learn more about Aptus Health's participation to the Privacy Shield Frameworks, please review Aptus Health's Privacy Shield policy: <https://aptushealth.com/privacy-shield>.

Finally, to ensure that your personal information does receive an adequate level of protection we have put in place the following appropriate measures to ensure that your personal information is treated by those third parties in a way that is consistent with and which respects applicable laws on data protection:

- Privacy and Data Protection Policies and Procedures
- Information Security Policies

- Privacy Training and Awareness Activities
- Processing Register/Data Inventory
- Initial Privacy Impact Assessment /Full Data Protection Impact Assessment processes Privacy and Security Incident Management and Data Breach Procedures
- Data Protection by Design/Default Processes
- Personnel Management Controls
- Third Party Compliance Assessment Controls

If you require further information about these protective measures, you can request it from the Compliance Team: [Complianceoffice@aptushealth.com](mailto:Complianceoffice@aptushealth.com).

## 11. 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. Details of these measures may be obtained from the Compliance Office at [ComplianceOffice@AptusHealth.com](mailto:ComplianceOffice@AptusHealth.com).

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.

## 12. Data retention

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

If we decide not to appoint you, we will retain your personal information for a period of up to 24 months after we have communicated to you our decision, unless you request us to destroy your personal information. We retain your personal information for that period so that we can show, in the event of a legal claim, that we have not discriminated against candidates on prohibited grounds and that we have conducted the recruitment exercise in a fair and transparent way. After this period, we will securely destroy your personal information in accordance with applicable laws and regulations.

If we wish to retain your personal information on file, on the basis that a further opportunity may arise in future and we may wish to consider you for that, we will write to you separately, seeking your explicit consent to retain your personal information for a fixed period on that basis.

In some circumstances we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you.

## 13. 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.

If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact [Complianceoffice@aptushealth.com](mailto:Complianceoffice@aptushealth.com).

## 14. Right to withdraw consent

When you applied for this role, you provided consent to us processing your personal information for the purposes of the recruitment exercise. You have the right to withdraw your consent for processing for that purpose at any time. To withdraw your consent, please contact [hrinternational@aptushealth.com](mailto:hrinternational@aptushealth.com). Once we have received notification that you have withdrawn your consent, we will no longer process your application and, subject to our retention policy, we will dispose of your personal data securely

## 15. Data protection officer

We have appointed a data protection officer (DPO) to oversee compliance with this privacy notice. If you have any questions about this privacy notice or how we handle your personal information, please contact the DPO at [dpo@aptushealth.com](mailto:dpo@aptushealth.com). You have the right to make a complaint at any time to Aptus Health's Lead Supervisory Authority, the *Commission Nationale de l'Informatique et des Libertés* (CNIL), the French supervisory authority for data protection issues.

## 16. Changes to this privacy notice

We reserve the right to update this privacy notice at any time. We may also notify you in other ways from time to time about the processing of your personal information.