Firstpoint Healthcare Ltd

Employment Business: GDPR privacy notice

Privacy notice

The Company is a recruitment business which provides work-finding services to its clients and work-seekers. The Company must process personal data (including special category data) so that it can provide these services – in doing so, the Company acts as a data controller.

You may provide your personal details to the Company directly, such as on an application form, by CV or via our website or we may collect them from another source such as a job board. The Company must have a legal basis for processing your personal data. For the purposes of providing you with work-finding services and/or information relating to roles relevant to you we will only use your personal data in accordance with the terms of the following statement.

This notice explains how Firstpoint Healthcare Ltd (referred to in this notice as **we, us** or **our**) collects and uses information during the work finding process. This notice covers the following:

What is personal data?

How do we collect personal data?

What information do we collect?

How do we use your information?

What is the legal basis that permits us to use your information?

What happens if you do not provide information that we request?

How do we share your information?

How do we keep your information secure?

All data is held on secure servers housed in a private suite within a Level(3) data centre. Access to the suite requires RFID access to the building, biometric fingerprint access to the floor the suite is on, and then a key code combination to access the private suite.

The internet breakout is secured using a Cisco firewall and we have Cyber Essentials accreditation for network security. All data is held on secure SAN nodes with RAID 10 redundancy, and data is accessible by authorised individuals only based on Active Directory and implemented windows security permissions.

All virtual servers are fully backed up nightly to a separate server within the private suite via Veeam software, and following this the backup is then replicated to a secure server housed at our Head Office in Stratford. External network access is limited to authorised users only, running Cisco AnyConnect VPN software via the Cisco ASA. All external access if via Windows RDP server access, with features such as printing to devices outside of the company network disabled.

We use the full Trend Micro Smart Protection Complete Suite, with all updates immediately deployed and enforced by our central Control Centre. All urgent windows security updates are automatically downloaded and deployed overnight by the Windows Server Update Service to ensure all servers and client machines are fully protected against latest threats. Practises employed to help secure company data include (but are not limited to):

Access to all data restricted to only authorised users.

- Endpoint encryption in place for portable media (including laptops)
- USB write blocking to prevent data being copied to personal drives
- Blocking of all web based email and data storage websites
- All users are required to change their password every 30 days
- All user passwords must meet minimum security requirements

- All machines auto lock after 10 minutes of inactivity to prevent unauthorised access to unattended machines

All hardware, backups, and data links are fully monitored 24/7 using PRTG Enterprise Console.

We will ensure access to personal data is restricted to employees working within our group on a need to know basis. Training will be provided to any employees working within the group who need access to your personal data to ensure it is secured at all times.

When do we transfer your information overseas?

For how long do we keep your information?

Your rights in relation to your information

Complaints

The Table at the end of this notice provides an overview of the data that we collect, the purposes for which we use that data, the legal basis which permits us to use your information and the rights that you have in relation to your information.

We may update this notice from time to time.

Contact details

Our contact details are as follows:

Address: Firstpoint Healthcare, Kingston House, Towers Business Park, Wilmslow Road, Manchester, M20 2LD
Telephone: 0121 643 5675

We have appointed a data protection officer who has responsibility for advising us on our data protection obligations. You can contact the data protection officer using the following details:

gdpr@firstpointhealthcare.com

What is personal data?

Personal data is any information that tells us something about you. This could include information such as your name, contact details, date of birth, and references.

How do we collect personal data?

We collect personal data about you from various sources including:

- from you when you contact us directly through the application and recruitment process;
- from other people when we check references or carry out background checks – if we do this we will inform you during the recruitment process of the checks that are carried out.
- Job boards

What information do we collect?

We collect the following categories of information about you:

- Personal contact details such as name, title, address, telephone number and personal email addresses
- Date of birth

- Equal opportunities monitoring information such as gender, race and ethnicity
- Recruitment information (including copies of right to work documentation, references, DBS, PIN number and other information in your CV or application form or otherwise provided as part of the registration process)
- Information about criminal convictions and offences committed by you
- Occupational Health information including COVID 19 vaccination status

How do we use your information?

We use your information for the following purposes:

- Supply work finding services
- To check you are legally entitled to work in the UK
- To assess your qualifications, experience and skills for a particular role or assignment
- To conduct data analytics studies to review and better understand job application rates
- To carry out equal opportunities monitoring
- Audits, as we operate in the healthcare industry we required to be audited by our clients to ensure legal and contractual compliance
- For payroll processing purposes
- To request or complete reference for work seeking opportunities
- Investigations for NMC or safeguarding referrals
- Occupational Health purposes

What is the legal basis that permits us to use your information?

Under data protection legislation we are only permitted to use your personal data if we have a legal basis for doing so as set out in the data protection legislation.We will process your personal data for the purposes of providing you with work-finding services. The legal bases we rely upon to offer these services to you are:

- Consent
- Contractual obligation
- Legal obligation
- Health or social care
- 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

The Table at the end of this notice provides more detail about the information that we use, the legal basis that we rely on in each case and your rights.

Some information is classified as "special" data under data protection legislation. This includes information relating to health, racial or ethnic origin, religious beliefs or political opinions, sexual orientation and trade union membership. This information is more sensitive and we need to have further justifications for collecting, storing and using this type of personal data. There are also additional restrictions on the circumstances in which we are permitted to collect and use criminal conviction data. We may process special categories of personal data and criminal

conviction information in limited circumstances with your explicit consent, in which case we will explain the purpose for which the information will be used at the point where we ask for your consent.

What happens if you do not provide information that we request?

We need some of your personal data in order to conduct the work finding services. If you do not provide such information, we may not be able to continue with the recruitment process or offer you employment/engagement.

How do we share your information?

We share your personal data in the following ways:

- Where we use third party services providers who process personal data on our behalf in order to provide services to us. This may include:
    - Clients in the Healthcare sector (we will seek your consent before providing your data to a client including COVID 19 vaccination status)
    - Our Occupational Health Provider
    - Auditors for our clients which include; Medacs, HTE framework (use Neuvens) and the CPP framework (use TIAA)
    - NMC
    - HMRC
    - Auto-enrolment pension provider
- We will share your personal data with third parties where we are required to do so by law or to comply with our regulatory obligations.
- 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
- If we sell any part of our business and/or integrate it with another organisation your details may be disclosed to our advisers and to prospective purchasers or joint venture partners and their advisers.

Where we share your personal data with third parties we ensure that we have appropriate measures in place to safeguard your personal data and to ensure that it is solely used for legitimate purposes in line with this privacy notice.

How do we keep your information secure?

All data is held on secure servers housed in a private suite within a Level(3) data centre. Access to the suite requires RFID access to the building, biometric fingerprint access to the floor the suite is on, and then a key code combination to access the private suite.

The internet breakout is secured using a Cisco firewall and we have Cyber Essentials accreditation for network security. All data is held on secure SAN nodes with RAID 10 redundancy, and data is accessible by authorised individuals only based on Active Directory and implemented windows security permissions.

All virtual servers are fully backed up nightly to a separate server within the private suite via Veeam software, and following this the backup is then replicated to a secure server housed at our Head Office in Stratford. External network access is limited to authorised users only, running Cisco AnyConnect VPN software via the Cisco ASA. All external access if via Windows RDP server access, with features such as printing to devices outside of the company network disabled.

We use the full Trend Micro Smart Protection Complete Suite, with all updates immediately deployed and enforced by our central Control Centre. All urgent windows security updates are automatically downloaded and deployed overnight by the Windows Server Update Service to ensure all servers and client machines are fully protected against latest threats. Practises employed to help secure company data include (but are not limited to):

Access to all data restricted to only authorised users.

- Endpoint encryption in place for portable media (including laptops)
- USB write blocking to prevent data being copied to personal drives
- Blocking of all web based email and data storage websites
- All users are required to change their password every 30 days
- All user passwords must meet minimum security requirements
- All machines auto lock after 10 minutes of inactivity to prevent unauthorised access to unattended machines

All hardware, backups, and data links are fully monitored 24/7 using PRTG Enterprise Console.

We will ensure access to personal data is restricted to employees working within our group on a need to know basis. Training will be provided to any employees working within the group who need access to your personal data to ensure it is secured at all times.

When do we transfer your information overseas?

When data is transferred to countries outside of the UK and the European Economic Area those countries may not offer an equivalent level of protection for personal data to the laws in the UK. Where this is the case we will ensure that appropriate safeguards are put in place to protect your personal data.

The countries to which your personal data is transferred and the safeguards in place are detailed below:

India

If you would like to see a copy of the adequacy mechanisms that we use to protect your personal data please contact gdpr@firstpointhealthcare.com

For how long do we keep your information?

As a general rule we keep personal data about candidates for the duration of the recruitment and selection process and for a period of:

- 12 months post registering
- 24 months post placement for working seeking services
- 6 years post placement for HMRC purposes

However, where we have statutory obligations to keep personal data for a longer period or where we may need your information for a longer period in case of a legal claim, then the retention period may be longer. Candidates are considered to be 'registered' when they have commenced the compliance process. No Personal Data will be retained for candidates that do not progress to the compliance stage.

Your rights in relation to your information

You have a number of rights in relation to your personal data, these include the right to:

- be informed about how we use your personal data;
- obtain access to your personal data that we hold;

- request that your personal data is corrected if you believe it is incorrect, incomplete or inaccurate;
- request that we erase your personal data in the following circumstances:
    - if we are continuing to process personal data beyond the period when it is necessary to do so for the purpose for which it was originally collected;
    - if we are relying on consent as the legal basis for processing and you withdraw consent;
    - if we are relying on legitimate interest as the legal basis for processing and you object to this processing and there is no overriding compelling ground which enables us to continue with the processing;
    - if the personal data has been processed unlawfully (i.e. in breach of the requirements of the data protection legislation);
    - if it is necessary to delete the personal data to comply with a legal obligation.
- ask us to restrict our data processing activities where you consider that:
    - personal data is inaccurate;
    - our processing of your personal data is unlawful ;
    - where we no longer need the personal data but you require us to keep it to enable you to establish, exercise or defend a legal claim;
    - where you have raised an objection to our use of your personal data;
- request a copy of certain personal data that you have provided to us in a commonly used electronic format. This right relates to personal data that you have provided to us that we need in order to take steps to enter into a contract with you and personal data where we are relying on consent to process your personal data;
- object to our processing of your personal data where we are relying on legitimate interests or exercise of a public interest task to make the processing lawful. If you raise an objection we will carry out an assessment to determine whether we have an overriding legitimate ground which entitles us to continue to process your personal data;
- not be subject to automated decisions which produce legal effects or which could have a similarly significant effect on you.

If you would like to exercise any of your rights or find out more, please contact gdpr@firstpointhealthcare.com. The Table at the end of this notice provides more detail about the information that we use, the legal basis that we rely on in each case and your rights.

Complaints

If you have any complaints about the way we use your personal data please contact gdpr@firstpointhealthcare.com who will try to resolve the issue. If we cannot resolve your complaint, you have the right to complain to the data protection authority in your country (the Information Commissioner in the UK).

Table: quick check of how we use your personal data

Purpose	Data used	Legal basis	Which rights apply?*
Work seeking services	Personal contact details, national insurance number, recruitment information, employment/engagement records, referencing, application form, DBS, vaccination status, PIN number and compensation history.	Legitimate interests. It is in our legitimate interests to evaluate whether you have the necessary experience, qualifications, skills and qualities to perform the relevant role. Necessary for the performance of the contract with you.	The generally applicable rights *plus the right to object*.
Right to work checks	Information relating to your right to work status, national insurance number, passport number, nationality, tax status information, and personal contact details.	Legitimate interest. It is in our interests to ensure that those who work for us have the right to work in the UK as well as to establish the statutory excuse to avoid liability for the civil penalty for employing someone without the right to undertake the work for which they are employed. Necessary for the performance of the contract with you.	The generally applicable rights plus the right to object.
Fraud and crime prevention	Information about criminal convictions and offences committed by you. Identity verification information.	Public interest and legitimate interest. It is in our interests as well as the interest of our candidates/ employees/ workers/ contractors to ensure the prevention of fraud and crime is monitored. This will ensure a safe workplace for all. Necessary for the performance of the contract with you.	The generally applicable rights plus the right to object.

Diversity monitoring	Gender, marital status and dependents and information about your race or ethnicity, religious beliefs, health, sexual orientation.	Public interest.	The generally applicable rights plus the right to object.
To deal with legal disputes	Personal contact details, references, information submitted as part of the selection process and interview notes.	Legitimate interest. It is in our interests to process personal data to make and defend legal claims to ensure that our legal rights are protected.	The generally applicable rights plus the right to object.
Investigations	Personal contact details, performance records, engagement records, PIN number	To comply with a legal obligation.	
Payroll processing	Personal contact details, National Insurance number, bank details, compensation	To comply with a legal obligation in terms of PAYE, NMW, HMRC and auto enrolment purposes. Legitimate interests. It is in our legitimate interests to ensure we process your remuneration correctly for the work you undertake and to ensure we fulfil our contractual obligations with you. Necessary for the performance of the contract with you.	The generally applicable rights plus the right to object
Audits	Personal contact details, recruitment information, employment/engagement records, referencing, application form, DBS, PIN number	Legitimate interests. It is in our legitimate interests to ensure we pass the audits as required by our Clients to ensure we remain as a supplier and provide work to you and other candidates. Necessary for the performance of the contract with you.	The generally applicable rights plus the right to object
Occupational Health Screening	Personal contact details, immunisations and vaccinations, health declaration	Legitimate interests. It is in our legitimate interests to ensure we comply with legal, NHS and contractual requirements to only provide workers who have been	The generally applicable rights plus the right to object

		assessed as ‘fit to work’ in a healthcare setting in a particular role. Necessary for the performance of the contract with you.
Referencing	Name, employment dates and any safeguarding or NMC investigations	Legitimate interests. It is in our legitimate interests to ensure we comply with legal, NHS and contractual requirements to only provide workers who have satisfactory clinical references. Necessary for the performance of the contract with you.

*The following generally applicable rights always apply: right to be informed, right of access, right to rectification, right to erasure, right to restriction and rights in relation to automated decision making. For more detail about your rights and how to exercise them please see **Your rights in relation to your information**