Data Protection Policy

Introduction

As a business, we are fully committed to compliance with the data protection requirements placed on us. We hold personal data about job applicants, temporary and agency employees, workers, clients, suppliers and other individuals for a variety of business purposes.

This policy sets out how we seek to protect personal data and ensure staff understands the rules governing their use of personal data to which they have access in the course of their work.

Scope

This policy applies to all staff, which for these purposes includes employees, temporary and agency workers, other contractors, interns and volunteers.

All staff must be familiar with this policy and comply with its terms.

We may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be circulated to staff before being adopted.

Definitions: In this policy -

business purposes	means the purposes for which personal data may be used by the business, (e.g. personnel, administrative, financial, regulatory, payroll and business development purposes, as well as allowing us to provide our services to our clients);
personal data	means information relating to identifiable individuals, such as job applicants, current and former employees, agency, contract and other staff, clients, suppliers and marketing contacts. This includes any expression of opinion about the individual and any indication of someone else's intentions towards the individual;
processing data	means obtaining, recording, holding or doing anything with data, such as organizing, using, altering, retrieving, disclosing or deleting it.

General principles

Our policy is to process personal data in accordance with the applicable data protection laws and rights of individuals as set out below. All staff has personal responsibility for the practical application of our data protection policy.

We will observe the following principles in respect of the processing of personal data:

- to process personal data fairly and lawfully in line with individuals 'rights;
- to make sure that any personal data processed for a specific purpose are adequate, relevant and not excessive for that purpose;
- to keep personal data accurate and up to date;
- to keep personal data for no longer than is necessary;
- to keep personal data secure against loss or misuse;
- not to transfer personal data outside the EEA (which includes the EU countries, Norway, Iceland and Liechtenstein) without adequate protection.

Fair and lawful processing

You should generally not process personal data unless:

- the individual whose details are being processed has consented to this;
- the processing is necessary to perform our legal obligations or exercise legal rights, or
- the processing is otherwise in our legitimate interests and does not unduly prejudice the individual's privacy.

The processing of clients 'personal data in order to provide the services they have requested from us will always be acceptable and you are free to do so without needing specific consent from clients.

However, you should still be mindful of your duties under this policy to keep such personal data safe and secure and you should consider whether you have the appropriate consent of the client before sharing any such personal data with a third party.

Accuracy, adequacy, relevance and proportionality

You should make sure data processed by you is accurate, adequate, relevant and proportionate for the purpose for which it was obtained. Personal data obtained for one purpose should generally not be used for unconnected purposes unless the individual has agreed to this or would otherwise reasonably expect the data to be used in this way.

Individuals may ask us to correct personal data relating to them which they consider to be inaccurate. If you receive such a request and do not agree that the personal data held is inaccurate, you should nevertheless record the fact that it is disputed and inform the Branch Manager. You must ensure that personal data held by the business relating to you is accurate and updated as required. If your personal details or circumstances change, you should inform YSP Job Solutions Ltd so our records can be updated.

Security

You must keep personal data secure against loss or misuse in accordance with our policies. It is everybody's responsibility to ensure that personal data remains secure and is not lost, misused or accidentally made available to a third party.

Where we use external organizations to process personal data on our behalf additional security arrangements need to be implemented in contracts with those organizations to safeguard the security of personal data. You should consult with the Branch Manager to discuss the necessary steps to ensure compliance when setting up any new agreement or altering any existing agreement.

Data retention

Personal data should not be retained for any longer than necessary. The length of time over which data should be retained will depend upon the circumstances including the reasons why the personal data were obtained. If you have questions as to how long certain data should be retained, you should contact the Branch Manager.

International transfer

You should not transfer personal data outside the EEA (which includes the EU countries, Norway, Iceland and Liechtenstein) without first consulting the compliance officer. There are restrictions on international transfers of personal data from the EEA to other countries because of the need to ensure adequate safeguards are in place to protect the personal data. If you are unsure of what arrangements have been or need to be put in place to address this requirement, you should contact the Branch Manager.

Rights of individuals

Individuals are entitled (subject to certain exceptions) to request access to information held about them. All such requests should be referred immediately to the Branch Manager. This is particularly important because we must respond to a valid request within the legally prescribed time limits.

You should not send direct marketing material to someone electronically (e.g. by email) unless:

- there is an existing business relationship with them in relation to the services being marketed; or
- we have their explicit consent to receive direct marketing from us.

You should abide by any request from an individual not to use their personal data for direct marketing purposes and should notify the Branch Manager about any such request. You should contact the Branch Manager for advice on direct marketing before starting any new direct marketing activity.

Reporting breaches

You have an obligation to report actual or potential data protection compliance failures to the Branch Manager.

This allows us to:

- investigate the failure and take remedial steps if necessary; and
- make any applicable notifications.

You may be concerned about reporting any data protection compliance failures, especially if you have made a mistake. However, as a company, we potentially have duties to notify the regulators and/or the individuals whose data has been compromised and a failure by you to report any compliance breach may put the company in breach of its obligations. It is therefore imperative that you report any breach, as soon as possible and credit will be given to you for doing so.

Consequences of failing to comply

We take compliance with this policy very seriously – our clients and other individuals that we deal with rightly expect that we will do so. Failure to comply puts both staff and the company at risk. The importance of this policy means that failure to comply with any requirement may lead to disciplinary action, which may result in dismissal.

If you have any questions or concerns about anything in this policy, you should not hesitate to discuss these with the Branch Manager.