Data Protection Policy

The Company takes the security and privacy of personal data seriously. We need to gather and use personal information or 'data' as part of our business, and to manage our relationship with our staff. We intend to comply with our legal obligations under the **Data Protection Act 2018** (the '2018 Act') and the **EU General Data Protection Regulation** ('GDPR') in respect of data privacy and security.

The Company obtains, stores and uses personal information (also referred to as data) about job applicants, current and former employees, temporary and agency workers, contractors, interns, and apprentices for a number of specific lawful purposes, as set out in the Company's data protection notices relating to recruitment and employment.

This policy sets out how we comply with our data protection obligations and seek to protect personal information relating to our staff. Its purpose is also to ensure that staff understand and comply with the rules governing the collection, use and deletion of personal information to which they may have access in the course of their work.

The Company's Data Protection Officer is responsible for informing and advising the Company and its staff on its data protection obligations, and for monitoring compliance with those obligations and with the Company's policies. Any questions or comments about this policy, or any requests for further information, should be directed to the Data Protection Officer who is responsible for data protection compliance within the Company. Any questions or comments about this policy, or any requests for further information, should be directed to them.

Staff should refer to the Company's Data Protection Privacy Notice for Employees, and where appropriate, to its other relevant policies which contain further information regarding the protection of personal information.

This policy does not form part of any contract of employment (or contract for services if relevant) and can be amended by the Company at any time. It is intended that this policy is fully compliant with the 2018 Act and the GDPR. If any conflict arises between those laws and this policy, the Company intends to comply with the 2018 Act and the GDPR.

Data Protection Principles

To comply with the Data Protection Principles set out in the 2018 Act the Company will ensure that all personal information it processes is:

- processed fairly, lawfully and in a transparent manner;
- collected and processed only for specified, explicit and legitimate purposes;
- adequate, relevant and limited to what is necessary for the purposes for which it is processed;
- accurate and kept up to date. We will take reasonable steps to ensure that any inaccurate data is deleted or rectified without delay;
- not kept for longer than is necessary for the purposes for which it is processed; and
- subject to appropriate technical and organisational measures to ensure that it is kept securely and protected against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

How we Define Personal Data

'**Personal data**' means information which relates to a living person who can be **identified** from that data (a '**data subject**') on its own, or when taken together with other information which is likely to come into the Company's possession. It includes any expression of opinion about the person and an indication of the intentions of us or others, in respect of that person. It does not include anonymised data.

This policy applies to all personal data whether it is stored electronically, on paper or on other materials.

Personal data might be provided to the Company by the employee or applicant, or someone else (such as a former employer, an employee's doctor, or a credit reference agency), or it could be created by the Company. It could be provided or created during the recruitment process or during the course of the contract of employment (or services) or after its termination. It could be created by a manager or other colleagues.

'**Special categories of personal data**' or '**sensitive data**' means personal data about an individual's race or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric data, health, or sex life and sexual orientation.

How we Define Processing

'Processing' means any operation which is performed on personal data such as:

- collection, recording, organisation, structuring or storage;
- adaption or alteration;
- retrieval, consultation or use;
- disclosure by transmission, dissemination or otherwise making available;
- alignment or combination; and
- restriction, destruction or erasure.

This includes processing personal data which forms part of a filing system and any automated processing.

Basis for Processing Personal Data

In relation to any data processing activity, there must be a legal basis for the processing consisting of one or more of the following:

(a) That the data subject has provided consent for the processing

(b) That the processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into the contract

(c) That the processing is necessary for compliance with a legal obligation to which the Company is subject

(d) That the processing is necessary for the protection of vital interests of the data subject or another natural person

(e) That the processing is necessary for the performance of a task carried out in the public interest or exercise of official authority

(f) That the processing is necessary for the purposes of the legitimate interests of the Company or a third party, and where those interests are not overridden by the interests or fundamental rights and freedoms of the data subject

We will only process personal data where we have a legal basis for doing so (see above), and, in the case of Special Category Data (see above), where one of the following special conditions applies:

- where it is necessary for carrying out obligations or exercising specific rights in the field of employment law;
- where it is necessary to protect the vital interests of a person where the subject is physically or legally incapable of giving consent;
- where the data has been made public by the subject;
- where processing is necessary for the establishment, exercise or defence of legal claims; and
- where processing is necessary for the purposes of occupational medicine or for the assessment of the working capacity of the subject.

In particular, we may use information in relation to:

- race, ethnic origin, religion, sexual orientation or gender to monitor equal opportunities;
- sickness absence, health and medical conditions to monitor absence, assess fitness for work, to pay benefits, and to comply with our legal obligations under employment law, including to make reasonable adjustments and to look after our employees' health and safety; and
- an individual's trade union membership to pay any subscriptions and to comply with our legal obligations in respect of trade union members

We do not take automated decisions about individuals using their personal data or use profiling.

Sharing Personal Data

We may share personal data with group companies or our contractors and agents to carry out our obligations under a contract of employment or for our legitimate interests. Such third parties include external payroll, HR or legal support.

We require those companies to keep such personal data confidential and secure and to protect it in accordance with the law and our policies. They are only permitted to process the data for the lawful purpose for which it has been shared and in accordance with our instructions.

We do not send personal data outside the European Economic Area. If this changes, individuals will be notified of this and the protections which are in place to protect the security of such data.

How Should you Process Personal Data for the Company?

Everyone who works for, or on behalf of, the Company has some responsibility for ensuring data is collected, stored and handled appropriately, in line with this policy.

The Company's Data Protection Officer is responsible for reviewing this policy and updating the Board of Directors on the Company's data protection responsibilities and any risks in relation to the processing of data. You should direct any questions in relation to this policy or data protection to this person.

- You should only access personal data covered by this policy if you need it for the work you do for, or on behalf of the Company and only if you are authorised to do so. You should only use the data for the specified lawful purpose for which it was obtained.
- You should keep personal data secure and not share it with unauthorised people.
- You should regularly review and update personal data which you have to deal with for work. This includes telling us if your own contact details change.
- You should not make unnecessary copies of personal data and should keep and dispose of any copies securely.
- You should use strong passwords, where applicable, and under no circumstances should you disclose these to others.
- You should lock your computer screens when not at your desk.
- Wherever possible, personal data should be encrypted before being transferred electronically to authorised external contacts.
- Consider anonymising personal data or using separate keys/codes so that the data subject cannot be identified.
- Do not save personal data to your own personal computers or any other personal device.
- Personal data should never be transferred outside the European Economic Area except in compliance with the law and with the authorisation of the Data Protection Officer.
- You should lock all drawers and filing cabinets which contain any personal data. Under no circumstances should you leave documents which include personal data in any place where they can be read by a person who does not have the authority to see the data. This includes your desk, in boxes, or in unlocked drawers or cabinets.
- You should not take personal data away from the Company's premises without authorisation from your line manager [or the Data Protection Officer]. Where you do have authority to take data from the office, you should avoid taking it in paper form, which is more difficult to secure, unless absolutely necessary. You should ensure that you take every reasonable precaution to ensure that personal data taken out of the office is kept safe, including: Protecting electronic data with a strong password, encrypting any memory stick or other portable storage device, not leaving laptops or bags in your vehicle, ensuring that no other people, including members of your family, have access to such information where it is taken home, avoiding taking such data on public transport unless absolutely necessary, in which case you should take the utmost care to ensure that such information is with your person at all times.
- Personal data should be shredded or disposed of securely (ie, confidential waste facilities) when you have finished with it.

You should ask for help from the Data Protection Officer if you are unsure about data protection or if you notice any areas of data protection or security you think the Company can improve upon.

Any deliberate or negligent breach of this policy by you may result in disciplinary action being taken against you in accordance with our disciplinary procedure.

It is a criminal offence to conceal or destroy personal data which is part of a subject access request (see below). This conduct would also amount to gross misconduct under our disciplinary procedure, which could result in your dismissal.

How to Deal with Data Breaches

A data breach may take many different forms, for example:

- Loss or theft of data or equipment on which personal data is stored;
- Unauthorised access to, or use of, personal data either by a member of staff or third party;
- Loss of data resulting from an equipment or systems failure;
- Human error, such as accidental deletion or alteration of data;
- Unforeseen circumstances, such as fire or flood;
- Deliberate attacks on IT systems, such as hacking, viruses or phishing scams.

Should a breach of personal data occur (whether in respect of you or someone else) then the Company must keep evidence of that breach. If the breach is likely to result in a risk to the rights and freedoms of individuals then we will notify the Information Commissioner's Office without undue delay and, where possible, within 72 hours of becoming aware of the breach.

If the breach is likely to result in a high risk to an individual's rights and freedoms, then we will notify the affected individual.

If you are aware of a data breach you **must** contact the Data Protection Officer immediately and keep any evidence you have in relation to the breach.

Subject Access Requests

Data subjects can make a '**subject access request**' ('SAR') to see the personal data the Company holds about them. This request must be made in writing. If you receive such a request, you should forward it immediately to the Data Protection Officer who will coordinate a response.

If you would like to make a SAR in relation to your own personal data you should make this in writing to the Data Protection Officer. The Company must respond within one month unless the request is complex or numerous, in which case the period can be extended by a further two months.

There is no fee for making a SAR. However, if your request is manifestly unfounded or excessive the Company may charge a reasonable administrative fee or refuse to respond to your request.

Data Subject Rights

An individual has the right to access information about what personal data the Company processes about them. You have the right to access your own personal data by way of a subject access request (see above). You can request that inaccuracies in your personal data be corrected. To do so you should contact your line manager in the first instance, or the Data Protection Officer where you are not satisfied with the response.

- You have the right to request that we erase your personal data where we are not entitled under the law to process it, or it is no longer necessary to process it for the purpose for which it was collected.

- While you are requesting that your personal data is corrected or erased or are contesting the lawfulness of our processing, you can apply for its use to be restricted while the application is made.
- You have the right to object to data processing where we are relying on a legitimate interest to do so and you think that your rights and interests outweigh our own and you wish us to stop.
- You have the right to object if we process your personal data for the purposes of direct marketing.
- You have the right to receive a copy of your personal data and to transfer your personal data to another data controller. We will not charge for this and will, in most cases, aim to do this within one month.
- With some exceptions, you have the right not to be subjected to automated decision-making.

In most situations the Company will not rely on your consent as a lawful ground to process your data. If it does request your consent to the processing of your personal data for a specific purpose, you have the right not to consent or to withdraw your consent later.

To exercise any of your rights, as outlined above, you should contact your line manager in the first instance, and if not satisfied with the response, you should contact the Data Protection Officer.

Simon Mansley
Managing Director
P&H Pipelines & Services Ltd
11th January 2021