



GENERAL DATA PROTECTION REGULATIONS POLICY FOR STAFF DATA

INTRODUCTION

Protecting your personal information is very important to us. As you know our businesses trust us to look after sensitive information about them, so it is only right that you are treated in the same way, as a valued employee.

This policy sets out how we use and protect your personal information in the workplace. The new GDPR Regulations take effect from 25th May 2018 and may change again in the future. They take the place of the previous data protection legislation. We have prepared for this and will update our arrangements on an ongoing basis.

DATA PROTECTION LAW

The new law takes data protection one step further in that it requires us to collect evidence of how we use your personal identifiable data (PID) and the steps we take to keep your PID safe.

We have to meet certain conditions and create processes and procedures which we have set out in this Policy.

The conditions are as follows:

- As your employer we will process PID in order to carry out our responsibilities and to provide you with information and services (i.e. payroll and pension administration)
- We will seek to comply with legislation and guidance at all times. In addition, we will process PID in order to provide information to Government and regulatory bodies, as required. This, as we have said, is our legitimate interest in your PID.

WHAT IS PERSONAL INFORMATION?

Personal information is personal identifiable data (also known as P.I.D) that can identify an individual.

Examples applicable to the workplace are:

- Name
- Address

- Telephone numbers
- Financial details i.e. Bank Account number
- Passport number
- Driving licence number
- National Insurance Number
- Tax details

WHERE DO WE GATHER YOUR INFORMATION FROM?

Our main source of such PID is yourself. You provide a lot of it when you apply for a job with us. You also notify us when your details change.

We also obtain, or are given, your PID from other sources i.e. HMRC and other Government Agencies

HOW DO WE USE YOUR PERSONAL INFORMATION?

We have what is termed a “legitimate interest” in holding your PID.

We use the PID that we hold to carry out our actions and duties as your employer. For example, we use your bank account details in order to pay your monthly salary into your account.

We use PID to run the Company in an efficient and appropriate way, for planning, training, business capacity, risk management, communication, governance, and audit.

Sometimes we will use PID for other agreed purposes e.g. a corporate event.

WHAT WILL WE NOT USE YOUR PID FOR?

Please be assured that we will never seek to profit from your PID and will never allow it to be collected for direct marketing purposes.

WHO DO WE SHARE YOUR PERSONAL INFORMATION WITH, AND WHY?

As your employer, and in addition to Government and Regulatory bodies, we need to share your PID with certain third party providers to the Company. Examples would be our payroll, and pension advisors.

We are taking all reasonable steps to obtain confirmation and evidence from these third parties that they take the same care with your PID as we do. This forms part of our due diligence as your employer and contributes to our business risk assessment process.

WHERE DO WE KEEP YOUR PERSONAL INFORMATION?

We keep your PID on paper files and databases. There is very restricted traceable access to both sources. Please see also the section on Security.

HOW LONG DO WE KEEP YOUR INFORMATION?

We will only keep your PID if there is a legitimate and provable reason for us to do so. This is what is termed our Legitimate Interest – i.e. that we are your employer. We follow retention policies set by legislation. PID in general is retained for up to 6 years after the termination of employment. Certain PID can be retained for a longer period i.e. for health and safety reporting purposes.

HOW DO WE DISPOSE OF YOUR INFORMATION?

When we dispose of your PID we do so either via permanent deletion of files held on our database, or via an independent firm who visit the premises and shred the papers off-site.

YOUR RIGHTS

The GDPR provides the following rights for individuals:

- The right to be informed about what your PID is being used for and by whom
- The right of access to the PID held about you (via a written Subject Access Request to which we have to respond within 1 month and for which we will not charge)
- The right to the correction of any inaccurate PID
- The right to withdraw or amend your consent to how we use your PID
- The right to erasure (i.e. the right to be forgotten)
- The right to restrict processing of PID
- The right to data portability (i.e. to have your PID sent to another organisation at your request)
- The right to object to how we are handling and storing your PID
- Rights in relation to automated decision making and profiling

WHAT DO YOU NEED TO DO ABOUT GDPR?

New employees will be asked to sign a GDPR Consent form as part of their pre-employment checks and induction. Current employees will also be asked to sign a Consent form.

Please keep your PID up to date by advising us of any changes in writing.

If you wish to amend, or withdraw, your consent to the use of all, or part of your PID, you should do so in writing, to your manager.

GDPR RISK ASSESSMENT

We will take all reasonable steps to obtain reassurance and evidence that any third parties who have access to your PID confirm to us that they adopt safe working practices for GDPR purposes.

The Company has taken professional advice with regard to GDPR preparation and will continue to follow advice and guidance in the future.

GDPR SECURITY ARRANGEMENTS

The offices of the Company are secure, with appropriate and robust security measures in place. PID is held on secure password and firewall protected databases. PID is not downloaded onto pen drives or laptops. If PID is in paper format, it is stored in lockable storage units, with restricted access. PID accessed by a Manager is not left unsupervised either on screen, or in a paper file.

IF THINGS SHOULD GO WRONG WHAT WILL WE DO?

In the unlikely event that there is ever a data breach the Company will follow the guidelines set out by the Information Commissioners Office. Certain data breaches have to be reported to the Information Commissioners Office.

Any data breach will be taken extremely seriously by the Company, whether it be by ourselves, or by a third party.

Immediate efforts will be made to contain and isolate the breach. A full investigation will take place with a report taken to the Board.

You will receive a full ongoing explanation and an impact assessment will be undertaken of your particular case.

ANY FURTHER QUESTIONS?

GDPR legislation is new to the UK. If you have any queries or concerns please raise them with your Manager. If we cannot provide an answer we will take professional advice and keep you informed.

Further information is also available from The Information Commissioner's Office:

First Contact Team,

Wycliffe House,

Water Lane,

Wilmslow,

Cheshire,

SK9 5AF

Helpline number: 0303 123 1113

Website address: <http://ico.org.uk>