Pride, Chartered Accountants (the company)

Data Protection Policy for Clients – Appendix to your terms of engagement

Introduction:

The General Data Protection Regulation (GDPR) became law on 24th May 2016. This is a single EU-wide regulation on the protection of confidential and sensitive information. It enters into force in the UK on the 25th May 2018, repealing the Data Protection Act (1998).

For the purpose of applicable data protection legislation (including but not limited to the General Data Protection Regulation (Regulation (EU) 2016/679) (the "GDPR"), and the Data Protection Act 2018 (currently in Bill format before Parliament) the company responsible for your personal data is Pride Accountants.

This Privacy Policy explains what we do with your personal data, whether we are in the process of providing you with a service, receiving a service from you, using your data to ask for your assistance in relation to one of our Clients, or you are visiting our website.

It describes how we collect, use and process your personal data, and how, in doing so, we comply with our legal obligations to you. Your privacy is important to us, and we are committed to protecting and safeguarding your data privacy rights.

This Privacy Policy applies to the personal data of our Website Users, Clients, Suppliers, and other people whom we may contact in order to find provide services to our clients.

Our company policy is to respect the privacy of clients and their employees and to maintain compliance with the General Data Protection Regulations (GDPR). Our policy is to ensure all personal data related to clients and their employees will be protected.

All employees and sub-contractors engaged by our company are asked to sign a confidentiality agreement. The company will, if required, sign a separate confidentiality agreement if the client deems it necessary. If a sub-contractor acts as a data processor for Pride Accountants an appropriate contract (art 24-28) will be established for the processing of your information.

You have the right to withdraw your consent to the processing of data. Please contact the Data Protection Officer in writing if you wish to withdraw your consent. If some circumstances we may need to store your data after your consent has been withdrawn to comply with a legislative requirement.

This policy complies with the General Data Protection Regulation and applied UK data Protection Legislation.

It is important to point out that we may amend this Privacy Policy from time to time.

If you are dissatisfied with any aspect of our Privacy Policy, please contact the Data Protection Officer.

You have legal rights and, where relevant, we have described these as well below.

This Privacy Policy applies in relevant countries throughout our international network. Different countries may approach data privacy in slightly different ways and so we also have country-specific parts to this Privacy Policy. You can find country-specific terms for your jurisdiction here. This allows us to ensure that we're complying with all applicable data privacy protections, no matter where you are.

Data Protection Officer:

The Company Data Protection Officer is David Whyle. Any queries or complaints should be addressed to him.

How do we safeguard your personal data?

We care about protecting your information. That's why we put in place appropriate measures that are designed to prevent unauthorised access to, and misuse of, your personal data.

Data:

The company will complete or update a ‘New client checklist form” with you upon our engagement and prior to commencement of work. You will be asked to supply personal information to the company for us to:

- contact you if required
- carry out the work you have engaged us to do
- to comply with regulatory requirements
- to comply with payroll, auto-enrolment and RTI requirements

We ask that you provide ID for copying to comply with our responsibilities under Money Laundering Regulations. You will be asked for ID if your circumstances change (i.e. change of address or change of surname) and/or periodically.

The above data is collected as a hard copy only and is not scanned electronically.

No business files are taken from the company premises, unless required to visit a client or their agents.

Electronic Copies:

Certain documents will be scanned onto our system; only signed copies will be retained as hard copies. The remaining paperwork will be shredded to DIN level 4 security requirements or pulped and disposed of.

Our computer systems are password protected and all staff are required to change their passwords on a regular basis.

The company uses “floating” laptops, which staff use for client visits. The laptops have data added to them whilst on client’s sites. When the staff member returns to the office, the data is removed from the laptop to an office computer and the laptop is wiped clean. The memory stick which is used to transfer the data is also wiped clean of data, as soon as the data has been transferred to an office computer.

No other data is stored on a removable device.

We back up data to an off-site secure server.

Payroll Services:

If you choose to use our payroll service, your employee details will be collected and added to our Sage payroll software. The information we require is:

Full name, address, date of birth, national insurance number, marital status, telephone numbers, email address and P45 or P46.

The reason we require this data is to process the payroll on your behalf and to comply with your payroll, auto-enrolment and RTI responsibilities.

If an employee leaves your employment, they will be deleted from the Sage payroll software in the following tax year.

Pensions:

If you choose to use our payroll service, we will have to liaise with your pension provider. Your employee’s data will be securely uploaded to your chosen pension provider via a secure web-based login.

You should request a copy of your pension providers Data Protection Policy directly.

Storage:

We will keep your business account details in a document wallet (this includes our working papers, final accounts, HMRC communications, copy bank statements, copy invoices, extracts from your records, etc.) which will be stored in a lockable cupboard on our company premises and to which only authorised staff members will have access to.

We will store the current year and previous years’ accounts, tax returns and associated paperwork only. Any older files will be archived for the statutory period of six years and securely stored electronically. All paper copies, with the exception of signed copies, are destroyed.

After the statutory period the electronic files will be disposed of securely.

Remote Access

In order to offer an efficient customer experience, our staff can access data remotely.

Access is password protected and passwords are changed every month or when an employee/ sub-contractor leaves the company.

Emails:

The company has a generic email system, where all emails can be accessed by any member of staff. If the email is addressed to a certain member of staff the email may still be seen by other members of staff. The reason for this is to ensure an efficient service and high quality customer care, if members of staff are out of the office.

All payroll, RTI and auto-enrolment communications will be sent and received by email.

A copy of your accounts, financial statements, personal tax information and associated correspondence will only be emailed to you following receipt of your specific request and authority.

Third Parties:

The company does not pass your data on to any third party, other than HMRC, Companies House, designated pension providers and financial and mortgage advisors subject to receipt of your authority.

Transparency and Choice:

You may at any time contact the company and ask what information we hold on your Company and its employees. You may ask us to update this information if it is incorrect, which we will endeavour to do as expediently as possible.

What do you do if you would like your own or your employee's data erased:

Please write to the Data Protection Officer if you wish for data to be erased. There may be circumstances where we are unable to do this immediately (to fulfil our and your legal responsibilities). We will advise you if these circumstances apply and when the data can be erased.

Information Security:

All data is password protected and only accessible by authorised company staff and sub-contractors. The company takes appropriate cyber security precautions.

How can you access, amend or take back the personal data that you have given to us?

Even if we already hold your personal data, you still have various rights in relation to it. To get in touch about these, please contact us. We will seek to deal with your request without undue delay, and in any event in accordance with the requirements of any applicable laws. Please note that we may keep a record of your communications to help us resolve any issues which you raise.

Right to object: If we are using your data because we deem it necessary for our legitimate interests to do so, and you do not agree, you have the right to object. We will respond to your request within 30 days (although we may be allowed to extend this period in certain cases). Generally, we will only disagree with you if certain limited conditions apply.

Right to withdraw consent: Where we have obtained your consent to process your personal data for certain activities (for example, carrying out work which you have engaged us to do), or consent to market to you, you may withdraw your consent at any time.

Data Subject Access Requests (DSAR): Just so it's clear, you have the right to ask us to confirm what information we hold about you at any time, and you may ask us to modify, update or Delete such information. At this point we may comply with your request or, additionally do one of the following:

- we may ask you to verify your identity, or ask for more information about your request; and
- where we are legally permitted to do so, we may decline your request, but we will explain why if we do so.

Right to erasure: In certain situations (for example, where we have processed your data unlawfully), you have the right to request us to "erase" your personal data. We will respond to your request within 30 days (although we may be allowed to extend this period in certain cases) and will only disagree with you if certain limited conditions apply. If we do agree to your request, we will Delete your data but will generally assume that you would prefer us to keep a note of your name on our register of individuals who would prefer not to be contacted. That way, we will minimise the chances of you being contacted in the future where your data are collected in unconnected circumstances. If you would prefer us not to do this, you are free to say so.

Right of data portability: If you wish, you have the right to transfer your data from us to another data controller. We will help with this – either by directly transferring your data for you, or by providing you with a copy in a commonly used machine-readable format.

Right to lodge a complaint with a supervisory authority: You have a right to complain to the UK supervisory Authority as below.

Information Commissioner:
Wycliffe house
Water Lane
Wilmslow
Cheshire
SK9 5AF

Tel: 01625 545745
www.informationcommissioner.gov.uk

If you would like to know more about your rights in respect of the personal data we hold about you, please contact the Data Protection Officer as above

Changes:

Our Data protection and Privacy Policy may change from time to time. We will not reduce your rights under this policy without your explicit consent. We will inform you of any Policy changes at the earliest opportunity.