SPIRE ACCOUNTANTS

Bookkeeping ~ Tax ~ Company Filings ~ Payroll

Data Protection Policy

Introduction

In the course of its business, the Spire Accountants ("the business") needs to gather and use certain information about individuals. This will include clients, suppliers and other business contacts, and employees and prospective employees, as well as other people that we have a relationship with, may need to contact, or with whom we need to deal.

This policy describes how this personal data must be collected, processed, transferred, handled and stored in order to meet the requirements of data protection law, in particular the General Data Protection Regulation (GDPR). We recognise that, not only must we comply with the principles of fair processing of personal data, we must also be able to demonstrate that we have done so. The procedures and principles set out below must be followed at all times by Spire Accountants, its employees and all those within its scope as set out below.

The policy applies to all employees and contractors who are provided with access to any of the files and/or computer systems. Collectively these individuals are hereafter referred to as 'users'. All users have responsibility for complying with the terms of this policy.

Personal Data

The GDPR regulates how organisations must collect, handle and store personal data. Personal data is any information relating to an identified or identifiable living individual. It is information which enables that person to be identified, directly or indirectly, and may include their name, address, telephone number(s), email address(es), age, location data, or online and biometric identifiers. We hold a wide range of information about clients, including highly confidential personal financial data such as their individual tax information.

These rules apply to all data stored in any structured way, including both paper files and electronically.

The Data Protection Principles

The GDPR contains a number of key principles which apply to the collection and processing of personal data and which underpin everything that follows:

1) Lawfulness, fairness and transparency
   Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.

2) Purpose limitation
   Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

3) Data minimisation
   Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

4) Accuracy.
   Personal data shall be accurate and, where necessary, kept up to date.

5) Storage limitation.
   Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

6) Integrity and confidentiality
   Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

7) Accountability
   The controller shall be responsible for, and be able to demonstrate compliance with the GDPR.

For the purposes of the law and these principles, a 'data controller' is a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed. In relation to the majority of our data, we are data controllers, although where we are responsible for looking after a client's payroll, they are the data controller and we are 'data processors'. A data processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. Our responsibilities as data processors are dealt with later in the Policy.

Our Responsibilities

The management at Spire Accountants are ultimately collectively responsible for ensuring that the business meets its legal obligations and that this Policy is followed.

The Data Protection Officer (DPO) has to do the following:

1) keeping our business partners updated about data protection responsibilities, risks and issues;
2) reviewing all data protection procedures and related policies, in line with an agreed schedule;
3) arranging data protection training and advice for everyone to whom this policy applies;
4) handling data protection queries from our business partners;
5) dealing with requests from anyone whose data we hold for access to that data (known as 'subject access requests');
6) checking and approving any contracts or agreements with third parties that may handle our personal data;
7) checking and approving any contracts or agreements with third parties whose personal data we may handle;
8) ensuring that policies on processing, retention, storage and deletion of data are adhered to and relevant documentation is maintained to evidence compliance;
9) ensuring that all systems, services and equipment used for storing data meet acceptable security standards;
10) performing regular checks to ensure that security hardware and software is functioning properly;
11) evaluating any third-party services the business is considering using to store or process data. For example, cloud computing services;
12) approving any data protection statements attached to communications such as emails and letters;
13) where necessary working with our business partners to ensure marketing initiatives are compliant with data protection principles and
14) ensuring that records of consents and withdrawal of consents to marketing are maintained.

Processing of Data

We are permitted to process data where one of the following legal bases applies:

1) the data subject has given their consent. An example might be where a client has agreed to be contacted about a new tax advice service we are providing;
2) the processing is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering a contract with them. An example of this is where we need to retain and file personal information about our clients in order to finalise their accounts or tax affairs, or where a potential client gives us their personal data in order for us to be able to quote for advice that they need, and in order for them to decide whether to instruct us;
3) the processing is necessary for compliance with a legal obligation to which the data controller is subject. An example of this might be where we pass personal data to the relevant money laundering authorities in a situation where we have an obligation to do so;
4) the processing is necessary to protect the vital interests of the data subject or another natural person. An example of this might be where we pass on information to the next of kin of an employee who is gravely ill;
5) the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller. This is usually used by public authorities carrying out vital functions such as provision of public utilities or public safety;
6) the processing is necessary for the purposes of legitimate interests pursued by the data controller or by a third party, except where those interests are overridden by the fundamental rights and freedoms of the data subject and their right to privacy in relation to their personal data. This is a difficult exception to generalise about, but it can be used by business where they have legitimate commercial aims which can override the data subjects' interests. An example might be the chasing of a legitimate customer debt. These legitimate aims may require some processing of personal data which may be justified in that context. Any user who wishes to use this basis would be advised to speak to the DPO to discuss it.

Sensitive Personal Data

This data has a special status under the law, as it is particularly personal in nature. It concerns a person's race, ethnicity, politics, religion, trade union membership, genetics, biometrics used for identification purposes, health, sex life or sexual orientation. There are a number of strict rules about the processing of this kind of data, and the kinds of situations in which it is legitimate to process it, and usually the data controller needs the data subject's explicit consent to do so or a clear legal basis. We will never disclose such data to any third party unless legally obliged to do so, and then only to appropriate authorities as required by law.

Data Processing

We act as data processors for a number of clients (the data controllers), receiving personal data relating to their employees and processing it for the purpose of payment of salary, and appropriate deductions. We do not expect to receive any data which is sensitive personal data in relation to this. We will:

1) only process the personal data provided in accordance with the data controller's instructions and in accordance with our contract with them;
2) implement technical and organisational measures in line with the GDPR to ensure the fair and lawful processing and the security of such data;
3) not disclose the data or transfer it to any third party without the explicit permission of the data controller, unless we are legally obliged to do or it is permitted and authorised by the contract with the data controller;
4) ensure that appropriate records are kept in order that we are able to demonstrate compliance with GDPR principles and
5) comply with our obligations to notify the regulatory authorities of any data breach.

Accountability and Record Keeping

Spire Accountants will keep written internal records of all personal data collection, holding and processing, and this will incorporate the following:

1) name and details of the business, its DPO and any third party data processors;
2) the purposes for which the business collects, holds and processes personal data;
3) details of the categories of personal data collected, held and processed by the firm and the categories of data subject to which the data relates;
4) details of any transfers of data to non-EEA countries including the mechanism for doing so and security measures taken;
5) details of the Spire Accountants retention policy (see Data Retention Policy) and
6) detailed descriptions of all technical and organisational measures taken by the business to ensure the security of personal data.

SPIRE ACCOUNTANTS

Bookkeeping ~ Tax ~ Company Filings ~ Payroll

Privacy by Design – Data Impact Assessments

Part of Spire Accountants duty is to ensure that in the planning of new processes or procedures which involve the use of personal data, we consider the impact of the changes and ensure that we have fully considered and complied with our obligations under the GDPR. The business will always ensure that all such changes are designed and implemented in accordance with the Regulation, and that the DPO is consulted and their recommendations are taken into account in the planning and introduction of such changes.

In any situation where new technologies are being deployed and the processing of the personal data is likely to result in a high risk to the data subjects' rights and freedoms under the Regulation, we will carry out a Data Impact Assessment, overseen by the DPO. This will deal with:

1) the type(s) of personal data that will be collected, held and processed;
2) the purpose for which it is to be used;
3) the business's objectives in processing this data and making this innovation;
4) how the personal data is to be used;
5) internal and external parties to be consulted;
6) why we need the data and how the collection of the data is proportionate to our need for it;
7) what risks there are for data subjects;
8) what risks the business (Spire Accountants) runs, and
9) what measures we are proposing to minimise and protect against the risks.

Providing Information to Data Subjects

We are required to ensure that, when we collect and process personal data, the data subject is aware of the purposes for which this is being done, and what is happening to the data. We therefore will ensure that the following principles are followed:

1) where we collect personal data directly from the data subject, we will inform them of the purpose for which it is being collected at the time of collection and
2) where we are obtaining personal data from a third party, we will inform the data subject why we are doing this.

Data Subject Access

'Subject Access Requests' (SARs), can be made by data subjects where an organisation holds personal data about them. This can be done at any time, and the requests are made in order for the data subject to find out what data is being held, and what is being done with it. Where a subject access request is being made to us as a payroll processor, we will refer the employee to the data controller (who is their employer or client) to deal with the request.

SARs should be:

1) made by the data subject in writing;
2) addressed to the DPO, who will deal with the request and
3) Spire Accountants will usually respond to them within one month, but we may need to extend it for a period of up to a further two months if it is a complex request or there are multiple requests. In that situation, the data subject(s) will be informed.

Spire Accountants will not charge the data subject any fee for responding to the SAR, unless the subject is asking for multiple copies of data already supplied or unless the request is manifestly unfounded or excessive.

Rectification of Personal Data

Where a data subject informs us that data we are holding about them is inaccurate or incomplete and requests that it is corrected, we will rectify the information and inform the data subject that we have done so, within one month of the request. Again, in complex cases, we may extend that period by up to two months.

Where the incorrect data is held by third parties to whom it has been disclosed, we will ensure that they are informed and that the data that they hold is rectified.

Erasure of Personal Data

Data subjects have a right to require Spire Accountants to erase personal data held about them when:

1) it no longer needs the data it is holding for the purposes for which it was originally collected;
2) the data subject wishes to withdraw their consent to the business holding and processing the data;
3) the data subject objects to the business holding and processing the data, and there is no overriding legitimate interest which allows us to continue to do so;
4) the personal data has been processed unlawfully and
5) the personal data needs to be erased in order for the business to comply with a particular legal obligation.

Where we are obliged to do so, we will erase the information and inform the data subject that we have done so, within one month of the request. Again, in complex cases, we may extend that period by up to two months, and again where the data is held by third parties to whom it has been disclosed, we will ensure that they are informed and that the data that they hold is erased.

Restriction of Personal Data Processing

Data Subjects have a right to request that the business ceases to process any personal data that we are holding about them. If that takes place, we will only retain whatever personal data we need to ensure that no further processing takes place, and we will inform any third parties to whom we have disclosed the data about the restriction on processing (unless it is impossible to do so or would involve disproportionate effort).

Objections to Personal Data Processing

Data subjects have a right to object to us processing their personal data based on our legitimate interests or for direct marketing purposes. Where the data subject notifies us of their objection, we will cease such processing immediately unless our legitimate interests override those of the data subject, or unless we need to continue to process the data in conducting a legal claim. Where the data subject is objecting to direct marketing, we will cease to use the data for this purpose immediately.

SPIRE ACCOUNTANTS

Bookkeeping ~ Tax ~ Company Filings ~ Payroll

Personal Data, Collected, Held and Processed

Type of Data	Purpose
Personal details of subcontractors, clients and suppliers such as names, addresses, contact details, age, sex etc	The administration of client work, subcontractor contracts and contracts with suppliers.
Financial Details of clients and prospective clients ie matters related to income and payroll, tax details, expenses claimed, court orders, pensions, insurance	To provide accountancy and related services to clients, in particular for the administration of their tax and personal financial affairs and to comply with both their and our legal obligations including in relation to tax and money laundering. To market our services to clients, in accordance with the GDPR
Payroll detail for employees of clients.	To provide payroll services to our clients and help them fulfil their payroll filing/reporting obligations.
Time recording of work for clients	To provide services to our clients and bill for them, to monitor performance of our subcontractors.

Data Security – Transferring Personal Data and Communications

We will ensure that we take the following measures with respect to all communications containing personal data:

1. all documents prepared for clients such as tax returns, and final accounts will be held in a separate client area, hosted by a reputable IT service provider. Access to the area is controlled;
2. all temporary files containing any personal data should be deleted without delay and
3. all personal data sent in hard copy form should be delivered to the recipient in person, in a container marked ‘Confidential’, or sent by recorded delivery or courier, as appropriate.

Data Storage and General Security

1. All electronic copies of personal data should be stored securely using privilege levels and passwords;
2. Regular password changes will be enforced and the number of logins will be restricted;
3. Passwords should never be written down or shared between any employees, agents, contractors or other persons working on behalf of the business, no matter what their level of seniority;
4. Computer equipment belonging to the business will be sited in a secure location within the office and in a position where they cannot be viewed by members of the public;
5. Computer terminals must not be left unattended, and should be logged off at the end of the session;
6. Personal data is backed up daily;
7. All software must be kept up to date;
8. Personal data should not be stored on any mobile device such as laptops, tablets and smartphones without the approval of the DPO and, where it is held, only in accordance with his or her instructions and limitations;
9. We will never transfer such data onto a device owned by a contractor or agent unless they have agreed to comply fully with the letter and spirit of this Policy and with the GDPR;
10. All manual files must be stored securely in locked cabinets and should not be left unsecured in the office overnight;
11. Computer print outs containing personal information should be destroyed without delay and should never be retained for scrap paper and
12. where personal data is to be erased, or otherwise disposed of, this will be done in accordance with the business's Data Retention Policy.

Organisational Measures

Spire Accountants will take the following steps in relation to the collection, holding and processing of personal data:

1. all contactors or other parties working on our behalf will be made fully aware of their individual responsibilities, and the responsibilities of the business, in relation to data privacy and the GDPR and they will be provided with a copy of this policy;
2. in respect of these individuals and of personal data held by the business:

    o only those persons who need access to particular personal data in order to complete their assigned duties will be granted such access;

    o all persons will be appropriately trained and supervised in handling personal data;

    o all persons will be encouraged to exercise caution in discussing work related matters within the workplace and

    o all contractors are bound by strict duties of professional confidentiality in discussing any work related matters outside the workplace, which will be adhered to and enforced.

3. where any agent, contractor or third party fails in their obligations under this Policy, we will ensure that they are required to indemnify us for costs, losses, damages or claims which may arise as a result.

Transfer of Personal Data outside the EEA

Spire Accountants may from time to time transfer personal data outside the EEA. This will only be done if one or more of the following applies to the transfer:

a) it is to a territory or sector within that territory that the European Commission has determined has an adequate level of protection for personal data, or appropriate safeguards as determined by the supervisory authorities;
b) it is made with the informed consent of the data subject;
c) it is necessary for the performance of a contract between the data subject and the business, or for pre-contractual steps taken at the request of the data subject and
d) it is necessary for important public interest reasons, or for the conduct of legal claims, or to protect the vital interests of the data subject.

Data Breach Notification

All personal data breaches must be reported immediately to the DPO.

If such a breach occurs, and it is likely to result in a risk to the rights and freedoms of data subjects eg financial loss, breach of confidentiality, reputational damage, the DPO is required to ensure that the ICO is informed without delay and, in any event, within 72 hours of the breach.

Where the breach is likely to result in a high risk to the rights and freedoms of data subjects, the DPO also needs to ensure that the data subjects affected by the breach are informed directly and without undue delay. The following information must be provided:

a) the categories and approximate numbers of data subjects affected;
b) the categories and approximate numbers of personal data records concerned;
c) the name and contact details of the business's DPO;
d) the likely consequences of the breach and
e) details of the measures taken, or proposed, to deal with the consequences of the breach.

Implementation of the Policy

This Policy is effective as of 12th June 2024.