Ian Richards & Co
Floor E Suite 7.5, Josephs Well,
Hanover Walk, Leeds LS3 1AQ
Telephone: 0113 2431506 Leeds
0207 1128347 London
Fax: 0113 3200350 Leeds
0207 1834350 London
Email: peterd@irichards.co.uk

May 2018

# Data Protection Policy

**Disclaimer**

This document is the product of a third party made available by Ian Richards & Co with the third party's express consent (the "Third Party Documentation"). The Third Party Documentation is not created or endorsed by Ian Richards & Co, its affiliates or its employees (the "Group") nor any business offering products or services through the Group. The provision of Third Party Documentation is for general informational purposes only and does not constitute a recommendation, solicitation or advice of any description. In addition, the Third Party Documentation is not intended to provide tax, legal or investment advice or represent the opinions of the Group. The Third Party Documentation is obtained from sources believed to be reliable and no guarantees are made by the Group or the providers of the Third Party Documentation as to its accuracy, completeness or timeliness. The Group shall not be liable for any action, inaction, decision or other transaction any person or entity may make based on their reliance on or use of Third Party Documentation and they do so at their own risk. There is no warranty of any kind express or implied regarding Third Party Documentation including but not limited to fitness for a particular purpose or non-infringement.

## Data Protection Policy

### Introduction

The firm has appointed Peter Duffy as the Head of Data Protection.

We have adopted a risk-based approach to data protection, whereby our policies and procedures only cover those areas which apply to our use of personal data. For example, as we currently do not use automated decision making or profiling then we do not have a policy on meeting the rights of data subjects with regard to automated decision making or profiling.

### Background

We are bound by relevant professional codes and regulations, including client confidentiality and the protection of client data.

## Personal data

Personal data includes any information related to a person that can be used to directly or indirectly identify the person. Such data includes, but is not limited to:

- Name
- Photo
- Email address
- Financial account details
- Social network posts
- Medical information
- IP address
- Passport number
- NI number

## Individual's rights

Individuals, also referred to as ‘data subjects’, have:

- the right to be informed;
- the right of access;
- the right to rectification;
- the right to erasure, sometimes referred to as the ‘right to be forgotten’;
- the right to restrict processing;
- the right to data portability;
- the right to object; and
- the right not to be subject to automated decision-making including profiling.

## Our obligations

Our obligations in respect of personal data include:

- We must have precise knowledge of the data we hold and process, its location, security usage and composition;
- We must identify if it is personal, prohibited, client-related or employee-related?
- How is it captured - is it permitted by law (‘lawful processing’) or consented to by the client?
- We must be able to provide information on how the data is used and on the rights of individuals regarding their data.
- We must demonstrate that we are managing personal data in a manner compliant with the regulations and be able to supply, on request, the details of the data we hold and how it has been used.
- We have to be able to erase every instance of an individual’s data in compliance with the right to be forgotten (including data held in backups).
- We must offer storage or conversion of data in a format that allows portability to other data processors.
- A duty to inform relevant parties if there is a breach.

## Our use of data

We process two different types of personal data: client data and firm data.

- ‘Client data’ is personal data received from clients in relation to professional engagements and practice.
- ‘Firm data’ is personal data held by a firm in relation to its own management, employees and affairs generally, including marketing databases.

When starting a new processing activity, we can only process personal data for the purpose for which it was provided.

## Training

All principals and staff receive:

- training (appropriate to their role) to ensure they understand these policies and procedures.
- details of any changes to the firm’s data protection policies and practices.
- training to refresh their understanding of these policies at least every two years.

An explanation of the firm’s policies and procedures is included in our induction procedures for new employees.

## Relationships with others - suppliers

When entering contracts with suppliers who process or store our data, we ensure that the supplier is fully compliant with the current data protection regime, and the contract addresses the requirements concerning the sharing of data.

The extent of the impact on our firm will depend on whether our firm is acting as a controller or processor.

A data controller is an organization that determines the purpose and methods for processing personal data. A data processor is an organization that processes personal data on behalf of a data controller.

We determine what information to obtain and process in order to do our work, so we may act as “controllers in common” or “joint controllers” with our clients.

## Relationships with others - clients

Our client terms and conditions reflect the firm’s data policies and practices.

When we act as the data processor, we must obtain documented instructions from any data controller on whose behalf we process data.

When we act as a joint controller, we must ensure the other joint controller complies with the regulations and that our contract in respect of the sharing of data is in compliance with the regulations.

## Data retention policies

### *What client data should we hold?*

The general principle is that we hold the minimum amount of data necessary.

The data we hold must be adequate, relevant and limited to what is necessary in relation to the purpose for which the data is processed. This applies to both automated personal data and manual filing systems where data is accessible.

### *How long do we retain personal data?*

In general, data should not be retained any longer than necessary for the task performed, or than is necessary to comply with the relevant laws and regulations.

We keep records and working papers for seven years from the end of the tax year, or accounting period, to which they relate or such longer period as the rules of self-assessment may require.

Under the anti-money laundering rules, we must keep records for five years after the relationship ends, and must delete any personal information obtained for the purposes of the anti-money laundering regulations after five years from the end of a business relationship unless:

- We are required to retain it under statutory obligation, or
- We are required to retain it for legal proceedings, or
- The data subject has consented to the retention.

Any decision to retain personal data beyond the policy noted above should be documented and approved by the Head of Data Protection. A decision to retain personal data beyond the policy above should consider:

- The current and future value of the information,
- The costs, risks and liabilities associated with retaining it; and
- The ease or difficulty of making sure it remains accurate and up to date.

## Privacy policies

We aim to ensure our privacy policies (also referred to as privacy notices) are clear, use plain language, are transparent and easily accessible.

Our privacy notices include:

- who we are;
- what we are going to do with the client information; and
- with whom it will be shared.

Our privacy notices also explain the lawful basis for processing, our data retention policies and the fact that individuals have a right to complain to the ICO if they think there is a problem with the way we are handling their data.

In addition, if we intend to use the client data in a way that is likely to be unexpected or objectionable, then this must be included in our privacy notices.

We communicate our privacy notices through our website, and our terms and conditions.

## Consent

Consent must be specific, informed, unambiguous, and freely given.

We record how and when customer consent was lawfully gained, including:

- Who consented
- When they consented
- What they were told at the time
- How they consented e.g. for written consent a copy of the relevant document
- Whether they have withdrawn consent, and if so when.

We recognise that “consent” is likely to degrade over time, and therefore we need to refresh the consent regularly in accordance with the context, the scope of the original consent and the individual’s expectations.

When obtaining consent, we do not rely on pre-checked boxes or implied consent. Instead, whenever data is collected on them, we require evidence of a positive “opt-in” by the individual separately from the firm’s standard terms and conditions. We also require an “opt-in” for direct marketing to prospective and existing customers.

When consent is withdrawn, we must notify other known holders of the data that consent has been withdrawn and that data should be erased.

## Employment issues

Employment contracts provide the lawful basis for processing personal data.

Our employment contracts include employees’ rights as data subjects. These include the right to be informed:

- they can make a complaint to the ICO (or relevant supervisory authority) if they believe their personal data is not being used appropriately or held securely.
- of the nature and reason for any monitoring by the firm of its employees; for example, by checking for excessive private use of telephones or e-mails, or inappropriate use of the internet.
- of their right to access information that the firm may hold on them. This includes information regarding any grievances or disciplinary action, or information obtained through monitoring processes. The firm must respond to such requests within 30 days. However, information can be withheld if releasing it would make it more difficult to detect crime or the information is about national security

The firm will require specific written consent from employees for one-off circumstances such as bank requests to confirm income for a mortgage application.

If the firm seeks to collect information regarding an employee's health, the employee’s consent will be sought. This information once collected will be held securely, with access limited to the appropriate principals.

## Breaches

A personal data breach is an accidental or unlawful act that has affected the confidentiality, integrity or availability of personal data. A personal data breach occurs whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals.

If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, we must also inform those individuals without undue delay.

Anyone who suspects they are the first person in the firm to identify a personal data breach must inform the Head of Data Protection, or in their absence, their own line manager.

Unless instructed to do so by the Head of Data Protection, or their appointed deputy, no one should attempt to resolve the problem themselves.

It is the responsibility of the Head of Data Protection to ensure that a register of all personal data breaches is maintained that records all breaches together with the firm's response to those breaches.

## Reporting personal data breaches

Any breach that is likely to result in a risk to the rights and freedoms of individuals must be reported to the Information Commissioner's Office within 72 hours.

If the firm is acting as data processors, we must inform the data controller as soon as feasibly possible and without undue delay.

Where we act as data controllers we must inform the individuals (data subjects) if there is a high risk that they will be impacted adversely by the breach. This must be as soon as feasibly possible and without undue delay.

## Subject Access Requests

Data subjects have the right to be informed, which includes the right to request the information held by the firm.

When the firm receives a Subject Access Request, it should be passed to the Head of Data Protection who will allocate responsibility for responding to the request to a relevant individual.

Unless the information requested would make it more difficult to detect crime or is a matter of national security, the firm must respond to any request within 30 days of receipt of the request. If we decide to refuse a request, we must tell the individual why and that they have the right to complain to the ICO and to seek a judicial remedy. Any refusal must be given without undue delay and at the latest, within one month of receiving the original request.

We will not make a charge for responding to Subject Access Request, unless the requests are manifestly unfounded or excessive.

It is the responsibility of the Head of Data Protection to ensure that a register of all Subject Access Requests is maintained that records all requests together with the date and nature of the firm's response to those requests.

**Monitoring**

The Head of Data Protection ensures that an annual critical review of the firm's compliance with its data protection policies and practices, as well as the effectiveness of those data protection policies and practices is carried out.

The Head of Data Protection will provide evidence of the annual compliance review to the principal responsible for completing the firm's annual practice assurance review.

After completion, the Head of Data Protection will provide a summary of the evidence of the annual compliance review to the next partners' meeting, together with details of any changes proposed to the firm's data protection policies and practices.