Data Protection Policy

Policy statement

Everyone has rights with regard to the way in which their **personal data** is handled. During the course of our activities as a provider of legal, advisory and consultancy services we will collect, store and **process** **personal data** about our clients, **workforce** and others. This makes us a **data controller** in relation to that **personal data**.

We are committed to the protection of all **personal data** and **special category personal data** for which we are the **data controller**.

The law imposes significant fines for failing to lawfully **process** and safeguard **personal data** and failure to comply with this policy may result in those fines being applied. Such breaches may also have significant regulatory and reputational consequences for the firm.

All members of our **workforce** must comply with this policy when **processing personal data** on our behalf. Any breach of this policy may result in disciplinary or other action.

We are committed to maintaining high standards of confidentiality in relation to the information provided to us in the course of our business and our organisational and technical measures are certified under ISO 27001 and accredited in relation to the UK Government's Cyber Essentials Plus security standards.

About this policy

The types of **personal data** that we may be required to handle include information about clients, our **workforce**, and others that we deal with. The **personal data** which we hold is subject to certain legal safeguards specified in the UK and Ireland Data Protection Acts 2018, the UK and EU GDPR and other regulations relating to the processing of personal data (together the '**Data Protection Legislation'**).

This policy and any other documents referred to in it set out the basis and rules on which we will **process** any **personal data** we collect from **data subjects**, or that is provided to us by **data subjects** or other sources.

This policy does not form part of any employee's contract of employment and may be amended at any time.

Definition of data protection terms

All defined terms in this policy are indicated in bold text, and a list of definitions is included in Annex A of this policy.

Responsibility for data protection

Our Legal Director - Risk & Compliance is responsible for ensuring compliance with the Data Protection legislation and with this policy. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the Legal Director - Risk & Compliance.

The Legal Director - Risk & Compliance is also the central point of contact for all **data subjects** and others in relation to matters of data protection.

Data protection principles

Anyone **processing personal data** must comply with the data protection principles. These provide that **personal data** must be:

- **Processed** fairly, lawfully and transparently in relation to the **data subject**;
- **Processed** for specified, lawful purposes and in a way which is not incompatible with those purposes;
- Adequate, relevant and not excessive for the purpose;
- Accurate and up to date;
- Not kept for any longer than is necessary for the purpose; and

- **Processed** securely using appropriate technical and organisational measures.

Personal Data must also:

- be **processed** in line with **data subjects'** rights;
- not be transferred to people or organisations situated in countries outside the UK without adequate protection.

We will comply with these principles in relation to any **processing** of **personal data** that we undertake. We set out how we will do this in our privacy notices, published on our website.

Fair and lawful processing

Data Protection Legislation is not intended to prevent the **processing** of **personal data**, but to ensure that it is done fairly and without adversely affecting the rights of the **data subject**.

For **personal data** to be **processed** fairly, **data subjects** must be made aware:

- that the **personal data** is being **processed**;
- why the **personal data** is being **processed**;
- what the lawful basis is for that **processing** (see below);
- whether the **personal data** will be shared, and if so with whom;
- the period for which the **personal data** will be held;
- the existence of the **data subject's** rights in relation to the **processing** of that **personal data**; and
- the right of the **data subject** to raise a complaint with the Information Commissioner's Office in relation to any **processing**.

We will only obtain such **personal data** as is necessary and relevant to the purpose for which it was gathered, and will ensure that we have a lawful basis for any **processing**.

For **personal data** to be processed lawfully, it must be **processed** on the basis of one of the legal grounds set out in the Data Protection Legislation. We will normally **process personal data** under the following legal grounds:

- where the **processing** is necessary for the performance of a contract between us and the **data subject**, such as an employment contract;
- where the **processing** is necessary to comply with a legal obligation that we are subject to, such as those that arise in relation to our accounts or our regulatory obligations;
- where the **processing** is necessary for our legitimate interests provided that these do not outweigh the rights and freedoms of the **data subject**. This will be the ground on which we rely for the majority of the work we do for clients that involves the **processing** of **personal data**; or
- where none of the above apply we will seek the consent of the **data subject** to the **processing** of their **personal data**. We will rely on consent for our marketing activities.

When **special category personal** data is being processed then an additional legal ground must apply to that processing. We will normally only **process special category personal data** under following legal grounds:

- where the **processing** is necessary for employment law purposes, for example in relation to sickness absence;
- where the **processing** is necessary for the establishment, exercise or defence of legal claims; or
- where none of the above apply then we will seek the explicit consent of the **data subject** to the **processing** of their **special category personal data**.

If any data user is in doubt as to whether they can use any **personal data** for any purpose, then they must contact the Legal Director - Risk & Compliance before doing so.

Legitimate Interests

As noted above, we will rely on this ground when processing personal data in connection with the provision of legal, advisory and consultancy services to our clients. In order to do so, we must undertake a 'Legitimate Interests Assessment' ("LIA").

Generally, each practice area will complete a high level LIA for the categories of activities they undertake that involve the processing of personal data, signed off at partner level. If any unusual or particularly intrusive processing is required in relation to a particular matter, an individual LIA should be carried out before that processing is undertaken.

Guidance should be sought from the Risk & Compliance Team in any cases where a data user is unsure as to whether or not a LIA is required.

Consent

Where none of the other bases for **processing** set out above apply then we must seek the consent of the **data subject** before **processing** any **personal data** for any purpose. We will ordinarily only rely on consent in relation to our marketing activities.

There are strict legal requirements in relation to the form of consent that must be obtained from **data subjects**.

If consent is required for any other **processing** of personal data of any **data subject**, then the form of this consent must:

- Inform the **data subject** of exactly what we intend to do with their **personal data**;
- Require them to positively confirm that they consent – we cannot ask them to opt-out rather than opt-in; and
- Inform the **data subject** of how they can withdraw their consent.

Any consent must be freely given, which means that we cannot make the provision of any goods or services or other matter conditional on a **data subject** giving their consent.

A record must always be kept of any consent, including how it was obtained and when.

Processing for limited purposes

In the course of our activities as a provider of legal, advisory and consultancy services, we may collect and **process** the **personal data** set out in our Schedule of Processing Activities. This may include **personal data** we receive directly from a **data subject** (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and **personal data** we receive from other sources (including, for example, our clients, central and local government, regulatory bodies, investigators and agents instructed by us or members of our **workforce**).

We will only **process personal data** for the specific purposes set out in our Schedule of Processing Activities or for any other purposes specifically permitted by Data Protection Legislation or for which specific consent has been obtained been provided by the data subject.

Notifying data subjects

Individuals have the right to be informed about how we use their personal information and we will inform them about about:

- our identity and contact details as **Data Controller** and those of the Legal Director - Risk & Compliance;
- the purpose or purposes for which we intend to **process** that **personal data** and the legal basis for the processing that we do;
- the categories of personal data we process;

- the categories of third parties with which we will share or to which we will disclose that **personal data**;
- whether the **personal data** will be transferred outside the United Kingdom ('UK') or Ireland, as applicable, and if so the safeguards in place;
- the period for which their **personal data** will be stored, by reference to our Retention and Destruction Policy;
- the existence of any automated decision making in the **processing** of the **personal data** along with the significance and envisaged consequences of the **processing** and the right to object to such decision making (although we do not at the present time undertake any such processing); and
- the rights of the **data subject** to object to or limit processing, request information, request deletion of information or lodge a complaint with the ICO (UK regulator) or Data Protection Commission (Irish regulator), as applicable.

This information is contained in our privacy notices. These are available on our website, links are provided to them from the emails we send and are referred to in our standard engagement letter and terms of business.

Adequate, relevant and non-excessive processing

We will only collect **personal data** to the extent that it is required for the specific purpose for which it was obtained, unless otherwise permitted by relevant Data Protection Legislation.

Accurate data

We will ensure that **personal data** we hold is accurate and kept up to date and will take reasonable steps to destroy or amend inaccurate or out-of-date data.

Data subjects have a right to have any inaccurate **personal data** rectified.

Timely processing

We will not keep **personal data** longer than is necessary for the purpose or purposes for which they were collected. We will take all reasonable steps to destroy, or erase from our systems, all personal data which is no longer required. Further information can be found in our Retention and Destruction Policy, including a Schedule that sets out retention periods in respects of the different categories of information that we hold.

When client matters are set up, a provisional date for closure is set based on the periods set out in the Schedule. The file is then returned or brought to the attention of the relevant fee earner around that date and a decision made as to whether the file has to be retained or can be destroyed.

Processing in line with Data Subject's Rights

We will process all **personal data** in line with **data subjects'** rights, in particular their right to:

- request access to any **personal data** we hold about them;
- object to the **processing** of their **personal data**, including the right to object to direct marketing;
- have inaccurate or incomplete personal data about them rectified;
- restrict processing of their **personal data**;
- have **personal data** we hold about them erased;
- have their **personal data** transferred; and
- object to the making of decisions about them by automated means.

Information about each of these rights is set out in Annex B. The issues are however often complex and as such all requests to exercise any of these rights must be referred to the Legal Director - Risk & Compliance. We must also notify any third party to whom we have disclosed the data of any rectification or erasure of that data.

Data security

We will take appropriate security measures against unlawful or unauthorised **processing** of **personal data**, and against the accidental loss of, or damage to, **personal data.**

We will put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction.

Any breaches of our data security measures, of this policy or of data protection legislation must be reported to the Legal Director - Risk & Compliance in accordance with our Notification and Reporting Policy.

The following policies set out the measures and controls we implement in order to maintain data security and the integrity of our systems and to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage:

- Acceptable Use Policy
- Information Security Statement
- Sending, Handling and Storing Confidential Information Policy
- Physical Access Policy
- Digital Access Policy
- Retention & Destruction Policy
- Notification & Reporting Policy

The information security procedures we adopt include:

Entry controls: Any stranger seen in entry-controlled areas should be reported in accordance with our Physical Access Policy.

Secure lockable desks and cupboards: Desks and cupboards must be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)

Document management: documents are managed in accordance with our Retention and Destruction Policy. This means that paper records are kept to a minimum and are scanned into one of our secure document management systems and securely destroyed where possible. Where we do need to keep hard copy documents such as Court bundles, these are locked away when not in use. Client documents such as deeds and wills are kept in our strongroom.

Methods of disposal: The Retention & Destruction Policy outlines the methods of secure record disposal.

Equipment: Data users must ensure that individual monitors do not show confidential information to passers-by and that they hibernate or log off from their laptop when not in use for extended periods or out of the office/home working environment. Devices may be locked if absent from secured offices/home workstations for shorter timeframes.

Document printing: Documents containing **personal data** must be collected immediately from printers and not left on photocopiers.

Any member of staff found to be in breach of the above security measures may be subject to disciplinary action.

Data Protection Impact Assessments

We take data protection very seriously and will consider and comply with the requirements of Data Protection Legislation in relation to all of our activities whenever these involve the use of personal data, in accordance with the principle of data protection by design and default.

In certain circumstances the law requires us to carry out detailed assessments of proposed **processing**. This includes where we intend to use new technologies which might pose a high risk to the rights of **data subjects** because of the types of data we will be **processing** or the way that we intend to do so.

We will complete an assessment of any such proposed **processing** and we have a template document which ensures that all relevant matters are considered.

The Risk and Compliance team should always be consulted as to whether a data protection impact assessment (DPIA) is required, and if so how to undertake that assessment.

Disclosure and sharing of personal information

We may share **personal data** that we hold about **data subjects**, and without their consent, with third parties such as regulatory bodies, the Courts, other law firms, experts and Counsel instructed by us, and other organisations and individuals where we have a lawful basis for doing so. Further information can be found in our privacy notices.

We will inform **data subjects** of any sharing of their **personal data** unless we are not legally required to do so, for example where **personal data** is shared for the purposes of, or in connection with, legal proceedings (including prospective legal proceedings), providing legal advice, or establishing, exercising or defending legal rights. We provide this information by way of our privacy notices.

Further detail is provided in our Records of Processing Activities.

Data Processors

We contract with various organisations who provide services to us including:

- Human resources providers, such as those who administer our payroll or carry out searches in relation to prospective staff;
- IT providers, such as those who administer our systems.

In order that these services can be provided effectively, we are required to transfer **personal data** of **data subjects** to these **data processors**.

Personal data will only be transferred to a **data processor** if they agree to comply with our procedures and policies in relation to data security, or if they put in place adequate measures themselves to our satisfaction. We will always undertake appropriate due diligence of any data processor before transferring the **personal data** of **data subjects** to them.

Contracts with **data processors** will comply with relevant legislation and contain explicit obligations on and expectations of the **data processor**.

Changes to this policy

We may change this policy at any time. Where appropriate, we will notify **data subjects** of those changes.

Annex A: Definitions

Term	Definition
Data	is information which is stored electronically, on a computer, or in certain paper-based filing systems
Data Subjects	for the purpose of this policy include all living individuals about whom we hold personal data. This includes pupils, our workforce, staff, and other individuals. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information
Personal Data	means any information relating to an identified or identifiable natural person (a data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person
Data Controllers	are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with Data Protection Legislation. We are the data controller of all personal data used in our business for our own commercial purposes
Data Users	are those of our Workforce whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times
Data Processors	include any person or organisation that is not a data user that processes personal data on our behalf and on our instructions
Processing	is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing also includes transferring personal data to third parties
Special Category	includes information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health or condition or sexual life, or genetic or biometric data.
Personal Data	Includes, any individual employed by us and partners and consultants who work with us
Workforce	are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with Data Protection Legislation. We are the data controller of all personal data used in our business for our own commercial purposes

Annex B: Rights of Individuals

Right of Access

Data subjects may request access to all **personal data** we hold about them. Such requests will be considered in line with our Subject Access Request Procedure.

Right to Object

In certain circumstances, **data subjects** may object to us **processing** their **personal data**. This right may be exercised in relation to **processing** that we are undertaking on the basis of a legitimate interest.

An objection to **processing** does not have to be complied with where we can demonstrate compelling legitimate grounds which override the interests, rights and freedoms of the **data subject** or is undertaken for the establishment, exercise or defence of legal claims. Such considerations are complex and must always be referred to the Legal Director - Risk & Compliance upon receipt of a request to exercise this right.

In respect of direct marketing, any objection to **processing** must be complied with and the processing must cease.

Right to Rectification

If a **data subject** informs us that **personal data** we hold about them is inaccurate or incomplete then we will consider that request and provide a response without undue delay and in any event within one month. If we consider the issue to be too complex to resolve within that period then we may extend the response period by a further two months. If this is necessary, then we will inform the **data subject** within one month of their request that this is the case.

Generally, we must comply with requests to rectify unless we are required to retain the data in its original form for the purposes of evidence. If that is the case, or if we are unable to ascertain whether the data is accurate or not, we must restrict the processing of the data. We should also include a note on the file of the request and our response to it. We may deal with incomplete data by the addition of a supplementary statement.

Right to Restrict Processing

Data subjects have a right to "block" or suppress the **processing** of **personal data** in certain circumstances. This means that we can continue to hold the personal data but not do anything else with it, save insofar as we have the data subject's consent to processing or processing is necessary for the establishment, exercise or defence of legal claims, for the protection of another person or in the public interest.

We must restrict the **processing** of **personal data**:

- In relation to a request for **personal data** to be rectified (see above);
- Where we are in the process of considering an objection to processing by a **data subject** and deciding whether our legitimate reasons for processing the data override those of the data subject;
- Where the **processing** is unlawful but the **data subject** has asked us not to delete the **personal data** but to restrict its processing instead; and
- Where we no longer need the **personal data** but the **data subject** has asked us not to delete the **personal data** because they need it in relation to the establishment, exercise or defence of legal claims.

If we have shared the relevant **personal data** with any other organisation, then we will contact those organisations to inform them of any restriction, unless this proves impossible or involves a disproportionate effort.

Right to Erasure: 'the Right to Be Forgotten'

Data subjects have a right to have **personal data** that we hold about them erased only in the following circumstances:

- Where the **personal data** is no longer necessary for the purpose for which it was originally collected;
- When a **data subject** withdraws consent to the processing – which will apply only where we are relying on the individuals consent to the processing in the first place, and where there is no other legal ground for the processing;
- When a **data subject** objects to the **processing** and there is no overriding legitimate interest to continue that **processing** – see above in relation to the right to object – or where the information is processed for direct marketing and the data subject has objected to that processing;
- Where the **processing** of the **personal data** is otherwise unlawful; or
- When it is necessary to erase the **personal data** to comply with a legal obligation to which we are subject

We are not required to comply with a request by a **data subject** to erase their **personal data** if the **processing** is taking place:

- To exercise the right of freedom of expression or information;
- To comply with a legal obligation or for the performance of a task in the public interest or in the exercise of our official authority;
- For public health purposes in the public interest;
- For archiving purposes in the public interest, research or statistical purposes; or
- For the establishment, exercise or defence of legal claims.

We will also tell other organisations about the erasure request if the personal data has been disclosed to others.

Right to Data Portability

In limited circumstances, a **data subject** has a right to receive their **personal data** in a machine readable format, and to have this transferred to other organisation.

If such a request is made, then the Legal Director - Risk & Compliance must be consulted.

Automated Decision Making & Profiling

The GDPR also has provisions on rights in relation to automated decision making and profiling, although this is unlikely to be relevant for our business. The GDPR restricts organisations from making solely automated decisions, including those based on profiling, that have a legal or similarly significant effect on individuals. As this is a high risk area, a Data Protection Impact Assessment (DPIA) must be completed.