



Mathieson Consulting Privacy Notice

This privacy notice applies to current or previous clients, prospective clients and associated parties, and explains how Mathieson Consulting Ltd (“we”, “us”, and “our”) process personal data.

The purpose of this Privacy Notice is to outline how we process personal data and the legal basis on which personal data is processed by us. It is important that those whose personal data we process read and understand this Privacy Notice.

Please note that this Privacy Notice provides an overview of how we process personal data and we may provide further information in just-in-time privacy statements during the course of your interactions with our people and services.

Data Controller

For the purposes of applicable data protection law, in particular the General Data Protection Regulation ("GDPR") and the UK GDPR, your data will be controlled by us as a subsidiary of the RBC Brewin Dolphin Group. We act as an independent data controller of your personal data in relation to providing services to you or communicating with you.

Sources of Personal Data

We collect personal data from you directly when acting as litigant in person or from third parties such as instructing solicitors, courts, pension administrators and pension providers.

Types of Personal Data

The type of personal data we collect will depend on the service we provide. We will only collect information that is adequate, relevant, and limited to what is necessary in relation to the purposes identified within this Privacy Notice.

The list below outlines the categories of personal data we may process, with common examples. Please note that this is an indicative, non-exhaustive list, and the personal data we use may change over time.

Data category	Common Examples
Personal Details	Biographical Contact details Gender Marital Status Internal client identification codes National identification numbers Family circumstances and background where relevant Behavioural and lifestyle Education and employment history Opinions, comments and feedback Signature
Financial Data	Current Financial Position Pension Scheme Information

	Tax Benefit Details Beneficiary of Will Information Billing
Special Category Data (Personal data revealing racial or ethnic origin. Political opinions. Religious or philosophical beliefs. Trade union membership. Genetic data and biometric data processed for the purpose of uniquely identifying a natural person.)	We usually don't handle special category data. However, if you or your legal representative give it to us, we'll determine if it's relevant to our processing purpose and whether we have a valid lawful basis to process it. If we don't then it will be deleted.
Anonymised Data	In addition to the categories of personal data described above, we produce anonymised and aggregated data and information that is not processed by reference to a specific individual
Cookies and technical data	We collect cookies from your device when you access and use our website.

Purposes of processing

Our primary purpose of processing personal data is to provide our services for litigants in person or by instructing solicitors.

The table below provides examples of the purposes for which we process personal data and the lawful basis we rely on under Article 6, Article 9 and Article 10 GDPR and UK GDPR. Please note that this is an indicative, non-exhaustive list.

Process	Purpose of processing	Lawful basis of processing
Fulfilling our actuarial and expert witness services	To take steps, as instructed, to collate, analyse and report on relevant data in line with family court directives for expert witnesses. To advise and provide commentary on legal and quasi-legal processes involved.	Article 6 (1) (b) – Performance of a contract Article 6 (1) (c) – Compliance with a legal obligation Article 6 (1) (f) – Legitimate interests
Management and administration of accounts, systems, services, products and offerings including via online and digital platforms	To effectively manage, administer and operate contractual arrangements and comply with instructions or requests on your behalf. To analyse and report on the effectiveness of our operations and growth strategies to increase efficiency, innovation and maintain a competitive edge.	Article 6 (1) (b) – Performance of a contract Article 6 (1) (c) – Compliance with a legal obligation Article 6 (1) (f) – Legitimate interests

	To administer charges	
Handling complaints, queries and legal claims	To respond to complaints, legal claims, data breaches or data protection rights requests	Article 6 (1) (c) – Compliance with legal obligation Article 6 (1) (f) – Legitimate interests Article (9) (2) (f) – Legal claims or judicial acts
Marketing and non-marketing communications	To send appropriate marketing communications that we think might be suitable for you or that we think is of importance, interest or relevance, including in response to requests from you via our webforms To ensure that where you have unsubscribed or ‘opted-out’ of certain communication types or channels, including marketing, we do not send such communications to you To notify you and associated parties about important changes to our services and provide non-marketing communications	<u>Marketing</u> Article 6 (1) (a) – Consent Article 6 (1) (f) – Legitimate interests <u>Non-marketing</u> Article 6 (1) (c) – Compliance with legal obligation Article 6 (1) (f) – Legitimate interests
Recording of telephone and video calls	For training, quality and product and service development and improvement To use as evidence in the event of a dispute or as evidence in court	<u>Article 6 (1) (f) – Legitimate interests</u>
Management and operations of technology and systems	To analyse, test, develop and improve our systems and services	<u>Article 6 (1) (f) – Legitimate interests</u>
Cookies and technical data	To collect, through our technology security services, traffic and security reports, information and activity logs on the usage of our systems and services. For example, websites visited by users, documents downloaded, security incidents and	<u>Article 6 (1) (a) – Consent</u> <u>Article 6 (1) (f) – Legitimate interests</u>

	<p>prevention measures taken by the gateway</p> <p>To collect, analyse and report on technical information about the services that you interact with when visiting our websites, applications and online advertisement.</p>	
--	---	--

Sharing Personal Data

We share personal data internally with our employees, agents and service providers and other companies within RBC, who are required to maintain the confidentiality of this information. Any transfer of personal data is based on a lawful basis, and we will only engage third parties that have appropriate technical and organisational measures to process, store, and safeguard personal data. While the third parties that we engage may change occasionally, the following table is an indicative, non-exhaustive list to help you understand the types of data sharing activities we undertake.

Third party	Purpose of sharing
Royal Bank of Canada (RBC) Group entities.	We are owned by Royal Bank of Canada (“RBC”) and we are part of the RBC Group. Where we have a valid business need, we will share data with other RBC Group entities, such as RBC Brewin Dolphin, to operate and manage shared services, systems and suppliers, request information about services and offerings provided by another entity, to conduct internal reporting and to co-operate in the investigation and response to complaints, legal claims, data breaches or rights requests.
Representatives	We may share information with authorised representatives acting on your behalf, such as a family member or legal representative.
Suppliers and vendors	We outsource certain functions to third party suppliers and vendors to assist with our business operations and may share certain types of personal data in the course of business. This may include accountants, professional advisers, IT and technical support providers, communications providers and specialist financial service providers and platforms.
Our business partners	We may share data with our business partners including intermediaries, financial advisers and pension or product/service providers, who provide you or your organisation with services alongside or related to those provided by us. Your information may be shared for the purpose of facilitating and hosting face-to-face and online events and webinars. We may also share information to co-operate in response to complaints, legal claims, regulatory authority requests, data breaches or data protection rights requests.
Government departments, bodies or agencies	We may disclose information to any court or tribunal or government, regulatory, law enforcement, fiscal or monetary authority or agency where reasonably requested to do so or if required by applicable law, regulations or guidelines or in order to resolve queries, concerns or complaints. For example:

	<p>HMRC National Crime Agency The police The Family Courts The Expert Witness Institute</p> <p>Recipients may also include tax, law enforcement and regulatory bodies, and courts and judicial bodies in other countries, such as the US, where applicable.</p>
Prospective buyers or sellers	<p>In the event we decide to sell any of our business or assets, or buy another business or its assets, we may share information for due diligence purposes. If we are acquired by a third party, personal data held by us about you will be disclosed to the third-party buyer.</p>
Debt collection agencies	<p>We reserve the right after notifying you to refer a debt, which you are unable or unwilling to pay, to a debt collection agency to recover our funds and any costs incurred to recover a debt, including legal costs. We also reserve a right, at our absolute discretion and without further notification, to sell the debt in its entirety to another party.</p>

International Transfers

For certain data processing operations your personal data will be transmitted through or stored or processed in other countries which are outside the UK and the European Economic Area.

These countries include:

- Guernsey
- Jersey
- Switzerland
- Canada; and
- United States of America

We will implement appropriate measures to ensure that your personal data remains protected and secure when it is transferred outside of your home country, in accordance with applicable data protection and privacy laws.

These measures include:

- **Adequacy Decisions:** We will ensure that the specific country provides an adequate level of protection to data privacy as approved by the UK and EU data protection authorities; or
- **Standard Contractual Clauses:** We will put in place a data transfer agreement with the recipient of the information using the contractual wording as approved by the UK and EU data protection authorities. For further information please contact us using the details at the end of this notice.

Data Transfers

The duration for which we retain your personal data will vary depending on the type of personal data and our reason for collection and processing. We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal

or reporting requirements. To determine the appropriate retention period for personal data, we consider the following:

- the volume of personal data
- the nature, and sensitivity of the personal data
- our obligations and legal requirements to retain your personal data
- the purpose of processing your personal data
- the risk of unauthorised use or disclosure of your personal data

Where we share data with RBC

RBC will retain the information we share with them for a period of seven years (or 11 years if the data controller of your personal information is located in Jersey) from the date of termination of your relationship with them, or for such other period as may be required from time to time under relevant laws and regulations, including those relating to record keeping and prescription periods. Such information may be retained after your account with them has been closed, and for customer identification purposes in accordance with their record keeping policy.

More information on how RBC manage your data can be found at <https://www.rbcwealthmanagement.com/en-eu/>

Security of personal data

We will take all appropriate technical and organisational steps to safeguard your personal data. In the unlikely event of a data breach, we will contact you in line with our legal obligations. Access to your personal data will be restricted to those who need to use it for legitimate legal and business purposes.

We follow several industry good practices to ensure this protection is fully effective and the appropriate technical and organisational measures are in place. All personal data is provided protection in line with security and data protection policies.

Data protection rights

The UK GDPR provides you, the data subject, with a number of rights when it comes to your personal data. On receipt of a valid request to invoke one of your rights, we will do our best to adhere to your request as promptly as reasonably possible.

Access: You have the right to request a copy of the personal data that we hold about you. There are exceptions to this right so that access may be denied if, for example, making the information available to you would reveal personal data about another person or if we are legally prevented from disclosing such information.

Accuracy: We aim to keep your personal data accurate, current, and complete. We encourage you to contact us to let us know if any of your personal data is not accurate or changes, so that we can keep your personal data up to date.

Objection: You have an absolute right to object to the processing of your personal data for direct marketing. Opting out of receiving marketing communications will not affect the processing of personal data for the provision of our services.

In other cases where the right to object applies, the right is not absolute and only applies in certain circumstances.

Restriction: You have the right to ask us to block or restrict the use of your personal data. The right is not absolute and only applies in certain circumstances.

Portability: You have the right to request to move, copy or transfer personal data from one IT environment to another in a safe and secure way, without affecting its usability.

Erasure: You have the right to ask us to erase personal data we hold about you. The right is not absolute and only applies in certain circumstances.

Right to withdraw consent: If you have provided your consent to the collection, processing and transfer of your personal data, you have the right to fully or partly withdraw your consent. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose(s) to which you originally consented unless there is another legal ground for the processing. If you withdraw your consent, this will not invalidate the lawfulness of any processing carried out on the basis of consent before you withdrew it.

Data Protection Complaints: If you believe that your data protection rights may have been breached, you have the right to lodge a complaint with the applicable supervisory authority or to seek a remedy through the courts.

Details of how to make a data protection rights request, query or to opt-out of marketing are below.

Contact Us

Making a data protection rights request

To exercise your rights or raise a query about the way we handle personal data, please email us at office@mcact.co.uk

Alternatively, write to us at:

81 Colmore Row,
Birmingham,
B3 2BA

Please provide as much detail as possible to help us deal with your request, such as the context in which we may have processed your information and the likely dates when we processed it. We may ask you to provide ID for identification and verification purposes. If you require any assistance, please email us at office@mcact.co.uk

Requests received by third parties on your behalf

If a request is submitted by a third-party representative (such as a solicitor) on your behalf, we may require additional documentation, such as a signed Letter of Authority.

Data Protection Complaints to the relevant Information Commissioner

You have the right to lodge a data protection complaint with the UK Information Commissioner's Office (ICO at <https://ico.org.uk>). However, we would be grateful for an opportunity to resolve matters with you in the first instance.

Changing your marketing preferences

If you would like to update your contact details or update any of your communication preferences, please get in touch with your usual contact at Mathieson Consulting Ltd or by using the above details.

Changes to this Privacy Notice

This Privacy Notice may be updated from time to time. Please check here for the most recent information on how we process your personal data.