PRIVACY POLICY

Contents

1. GENERAL APPROACH TO DATA PRIVACY

1.1 TWM Solicitors LLP and its associated companies, TWM Trust Corporation Limited and TWM Corporate Services Ltd, (collectively referred to as "TWM") hold a significant amount of confidential information about *Clients* and third parties, and is committed to the highest standards of data protection. This policy sets out TWM's approach to handling the *Personal Data* of our *Clients*, suppliers, contractors, contacts, and other third parties.

1.2 Please refer to the Glossary in Schedule 1 for the definition of words and expressions used in italics in this Policy.

1.3 Schedule 2 to this Policy sets out the categories of information we hold in relation to our *Clients and the lawful basis for doing so*.

1.4 TWM retains information for the periods set out in Schedule 3. These periods reflect our data protection obligation not to keep personal data for longer than is necessary, and also our statutory, regulatory and business needs to keep records. The firm will review these retention periods at least every five years, or more frequently if there are changes in limitation periods or statutory obligations as to the retention of records.

1.5 Schedule 4 to this Policy sets out the Rights of *Data Subjects.*

1.6 TWM reserves the right to update this policy at any time without express notice to any third party, so please check our website regularly for the latest version of this Privacy Policy. We last revised this document in August 2022.

2. PERSONS WITH RESPONSIBILITY

The person with overall responsibility for this policy is the firm's Managing Partner, Compliance Officer for Legal Practice (COLP) and *Data Protection Officer ("DPO*"), Jamie Berry. The DPO has overall responsibility for data protection, privacy and information management, and this Policy. Please contact our *DPO* if you have any questions about this Policy.

3. OUR OBLIGATIONS

3.1 When we hold information about identifiable people (known as "*Data Subjects*") this gives rise to obligations under the *Data Protection Legislation*. TWM is a *Data Controller* for the purposes of this legislation.

3.2 *Data Subjects* have rights if we hold information about them. These include the right to be informed what we hold, the right to have errors corrected and the right to have *Personal Data* deleted if we have no justification for holding it.

4. GROUNDS FOR *PROCESSING PERSONAL DATA*

4.1 The *DPA* allows *Processing* for specific purposes. Those which most often apply are that the *Processing* is necessary:

(a) for the performance of a contract to which the *Data Subject* is a party, or to take steps at the *Data Subject's* request before entering into such a contract;

(b) for compliance with a legal obligation other than a contractual obligation to the *Data Subject*;

(c) to protect someone's vital interests;

(d) for our *Legitimate Interests*, or those of a third party, where such interests are not overridden by the interests or rights of the *Data Subject*.

4.2 We do not need *Consent* to *Process Personal Data* in any of the cases listed in paragraph 4.1. In other cases, for example, direct marketing (see section 7 below), we may need *Consent*. We do not ask for *Consent* if we do not need it.

4.3 The *Processing* of *Sensitive Personal Data* is subject to stricter conditions. The usual grounds on which we are entitled to *Process Sensitive Personal Data* are:

(a) *Explicit Consent* of the *Data Subject;*

(b) it is necessary to protect the vital interests of a *Data Subject* who is physically or legally incapable of giving *Consent*;

(c) the *Personal Data* was manifestly made public by the *Data Subject*;

(d) it is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity;

(e) it is necessary for the purposes of carrying out the obligations and exercising specific rights of the *Data Controller* or of the *Data Subject* in the field of employment and social security and social protection law; and/or

(f) it is necessary for occupational health reasons or for the assessment of working capacity of *Personnel.*

4.4 We will do our best to ensure that the *Personal Data* we *Process* is accurate, complete, kept up to date and relevant to the purpose for which we collected it. We will do our best to check the accuracy of any *Personal Data* at the point of collection and at regular intervals afterwards and, subject to our overriding legal and professional obligations, we will take all reasonable steps to destroy or amend *Personal Data* which we know to be inaccurate or out of date.

4.5 We will not *Process Personal Data* for purposes other than those for which we originally collected it, unless we reasonably consider that we need to use it for another purpose which is compatible with the original purpose.

4.6 If we need to *Process Personal Data* for a purpose which is new, different or incompatible with that which was disclosed when we first obtained the *Personal Data*, we will inform the *Data Subject*, explain the legal basis which allows us to do so and, in some cases, obtain the *Data Subject's Consent*. Similarly, if the *Data Subject* requires an explanation as to how the *Processing* for the new purpose is compatible with the original purpose, we will provide it.

4.7 Please note, however, that there are many situations where, as solicitors, we are required or permitted by law to *Process Personal Data*, in compliance with the above rules, without the knowledge or *Consent* of the *Data Subject*.

5. WHAT PERSONAL DATA WE COLLECT AND HOW WE USE IT

5.1 In Schedule 2, we have set out a description of the different types of *Personal Data* we may collect, use, store and transfer, the ways we plan to use the *Personal Data*, and the legal justification on which we rely in order to do so. Where we rely on the justification that it is necessary to *Process* the *Personal Data* for our *Legitimate Interests* we have also, where appropriate, identified what we consider those *Legitimate Interests* to be.

5.2 Depending on the specific purpose for which we are *Processing* the *Personal Data*, more than one legal justification may apply. Where more than one legal justification is given in Schedule 2, *Data Subjects* who require more information about the specific legal justification on which we are relying to *Process* their *Personal Data* may contact us and request an explanation.

6. COOKIES AND OTHER PERSONAL DATA COLLECTION METHODS

6.1 We collect *Personal Data* from and about our *Clients*, contacts, *Personnel*, and other third parties by various different methods, including through:

(a) <u>Cookies, automated technologies or interactions</u>

As users interact with our website, we may automatically collect technical data about their equipment, browsing actions and patterns. We collect this *Personal Data* by using cookies, server logs and other similar technologies.

TWM's website uses cookies to distinguish between users of our website. This helps TWM to provide individual users with a good experience when they browse our website and also allows us to improve our site.

A cookie is a small file of letters and numbers that we store in a user's browser or the hard drive of their computer if they provide their *Consent*. Cookies contain information that is transferred to a user's hard drive.

We use the following cookies:

- Strictly necessary cookies. These are required for the operation of our website. They include, for example, cookies that all users to log into secure areas of our website or make use of e-billing services;

- Analytical/performance cookies. These allow us to recognise and count the number of visitors and to see how visitors move around our website. This helps us to improve the way our website works, for example by ensuring that users can find what they are looking for easily.

We may also receive technical data about our *Clients*, contacts and other third parties if they visit other websites employing our cookies.

TWM uses Google Analytics to collect the above information. These cookies collect information in anonymous form. For further details please visit: https://support.google.com/analytics/answer/6004245

Users can block all or some cookies by adjusting the settings on their browser. However, if they set their browsers to disable or refuse cookies (including essential cookies) users may not be able to access all or parts of our website. To opt out of Google Analytics please visit https://tools.google.com/dlpage/gaoptout

(b) Direct interactions

They may give us their identity, contact and/or financial data by filling in forms, giving us their business card, or by corresponding with us by post, telephone, email or otherwise. This includes *Personal Data* they provide when they:

- become *Clients* of TWM;
- seek information about our products or services;
- create an account on our website;
- subscribe to our service or publications;
- request marketing to be sent to them; and/or
- give us feedback.

(c) Third parties or publicly available sources

We may receive *Personal Data* from various third parties and public sources as set out below:

- Technical Data from parties such as analytics providers, eg Google Analytics based outside the *UK*; and search information providers eg SmartSearch based inside the *UK*;
- Contact, financial and transaction data from providers of technical, payment and delivery services such as lending institutions based inside the UK;
- Identity and contact data from publicly availably sources such as Companies House and the Electoral Register based inside the UK;
- Identity, contact, financial data from benefits providers/brokers based inside the *UK;*
- Identity, contact and financial data from our payroll provider based inside the UK;
- Identity, contact, financial and recruitment data from recruitment agencies and job sites based inside the UK.

7. MARKETING

7.1 We use identity, contact, technical, usage and profile data about our *Clients*, contacts or other third parties to form a view on what we think they may want or need, or what may be of interest to them, and to:

(a) send them occasional newsletters;

(b) tell them about relevant changes in the law;

(c) tell them about services that we provide; and/or

(d) send them invitations;

which we think may be relevant to them.

7.2 We are able to do this without express *Consent* if they have provided us with their Contact Data in the course of a previous instruction, or when requesting information from us about the services we offer so long as we give them an opportunity to opt out of receiving such marketing communications in the first and in each subsequent communication, and they have not done so. Otherwise, we will not send marketing communications to anyone who has not expressly *Consented*.

7.3 We will not share *Personal Data* with any third party for marketing purposes without the express *Consent* of the *Data Subject*.

7.4 *Clients*, contacts and other third parties may ask us to stop sending them marketing communications by contacting us at any time.

7.5 If *Clients* or contacts opt out of receiving marketing communications from us at any time, their details will be suppressed as soon as possible. This involves

retaining just enough information to ensure that marketing preferences are respected in the future.

7.6 If *Data Subjects* change their mind about receiving marketing communications from us, they can update their choices at any time by contacting us.

8. SHARING PERSONAL DATA

8.1 We may have to share *Personal Data* with third parties for the purposes set out in the table in Schedule 2.

8.2 We will only share the *Personal Data* we hold within the firm if the recipient has a matter-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions.

8.3 We may need to share *Personal Data* with external third parties, such as:

(a) Professional advisers, acting as *Process*ors or joint controllers, including lawyers, bankers, auditors who provide consultancy, banking, legal, insurance and accounting services;

(b) HM Revenue & Customs, regulators and other authorities, acting as *Process*ors or joint controllers, based in the UK who require reporting of *Processing* activities in certain circumstances;

(c) The Law Society, the Solicitors Regulation Authority, and the Legal Ombudsman; and

(d) Banks, other lending/mortgage institutions, lending/mortgage brokers, insurers, and insurance brokers.

8.4 We will only share the *Personal Data* we hold with third parties, such as our service providers if:

(a) they have a need to know the information for the purposes of providing the contracted services (eg when instructing Counsel, or dealing with TWM's benefits providers/brokers);

(b) sharing the *Personal Data* complies with this Policy and the *Data Subject's Consent*, if required, has been obtained;

(c) the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;

(d) the transfer complies with any applicable cross border transfer restrictions; and

(e) a fully executed written contract that contains *DPA* approved third party clauses has been obtained or is published on their website.

8.5 We require all third parties to respect the security of the *Personal Data* relating to our *Clients* and to our *Personnel* and to treat it in accordance with the law.

We do not allow our third party service providers to use *Personal Data* relating to our *Clients* and to our *Personnel* for their own purposes and only permit them to *Process* such *Personal Data* for specified purposes and in accordance with our instructions.

8.6 We may share *Personal Data*, in strict confidence, with third parties with whom we may be contemplating acquiring parts of their business or assets, merging with them or selling, transferring, or merging parts of our business or assets. In such cases, any new owners of the business may *Process Personal Data* in accordance with this Policy.

9. SENDING DATA OUTSIDE THE UK (SEE ALSO SECTION 8 – SHARING PERSONAL DATA)

9.1 We will only send a *Data Subject's Personal Data* outside of the UK to:

9.1.1 follow a *Client*'s instructions eg their matter involves a foreign property transaction; or a matrimonial matter where the other party or children live in another country;

9.1.2 comply with a contractual, regulatory or legal duty;

9.1.3 work with our agents or advisers who we may use to assist in fulfilling your instructions eg estate agents, Counsel, etc; and/or to

9.1.4 enforce our contractual rights and remedies against *Clients* outside the UK.

9.2 If we do transfer information to our agents or advisers outside of the *UK*, we will ensure a similar degree of protection is afforded to it by putting in place at least one of the following safeguards:

9.2.1 only transferring it to a countries outside the UK that have been deemed to provide an adequate level of protection for personal data*;*

9.2.2 putting in place an agreement with the recipient that means they must protect it to the same standards as is required in the *UK* or ensuring their existing procedures are compliant; or

9.3 More information in relation to the points above can be found on the Information Commissioner's website.

10. DATA RETENTION

10.1 We will not keep *Personal Data* in a form which permits the identification of the *Data Subject* for longer than is necessary for the legitimate business purpose or purposes for which it was originally collected, or for the purpose of satisfying any legal, accounting or reporting requirements.

10.2 In some circumstances, *Data Subjects* may ask us to delete *Personal Data* we hold relating to them. We do not always have to comply with such requests,

and it is not always possible to do so. In some circumstances, we may *Pseudonymise Personal Data* (so that it can no longer be associated with a *Data Subject*) for research or statistical purposes, in which case we may use the *Pseudonymised Personal Data* indefinitely without further notice to the *Data Subject*.

10.3 Schedule 3 to this *Policy* sets out the periods for which *Personal Data* is stored. TWM aims to ensure that, subject to overriding legal and regulatory requirements, *Personal Data* is deleted when no longer reasonably required for the purposes for which it was being held. By law we have to keep basic information about our *Clients* (including Contact, Identity, Financial and Transaction Data) for a minimum of six years after they cease being *Clients*, and often for much longer.

10.4 We take all reasonable steps to destroy or erase from our systems all *Personal Data* that we no longer require.

11. DATA SUBJECTS' RIGHTS AND REQUESTS

11.1 *Data Subjects* have rights when it comes to how we handle their *Personal Data*. A notice to *Data Subjects* setting out their rights is out in Schedule 4.

11.2 TWM will verify the identity of an individual requesting *Personal Data* under any of the rights listed above and will not allow third parties to persuade us to disclose *Personal Data* without proper authorisation.

11.3 It should be noted that for regulatory, professional indemnity and other professional reasons (eg conflict checking or dealing with any future claims or complaints relating to a *Client*'s matter), we will not delete a *Client*'s matter from the firm's case management and email systems for a minimum of 10 years, and therefore all *Personal Data* provided in order for us to fulfil our *Client*'s instructions will be retained. Non-germane information provided (eg a *Client*'s personal interests or non-relevant family information) will be deleted.

Jamie Berry

Managing Partner/COLP/DPO

October 2023

SCHEDULE 1

DEFINITIONS OF TERMS USED

***Automated Processing*:** any form of automated *Processing* of *Personal Data* consisting of the use of *Personal Data* to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

***Client*:** a person or organisation using the services of TWM where that person or organisation has signed or otherwise accepted our Terms of Business.

***Consent**:* agreement which must be freely given, specific, informed and be an unambiguous indication of the *Data Subject*'s wishes by which they, by a statement or by a clear positive action, signifies agreement to the *Processing* of *Personal Data* relating to them.

Data Controller: the person or organisation that determines when, why and how to *Process Personal Data*. It is responsible for establishing practices and policies in line with the *GDPR*. We are the *Data Controller* of all *Personal Data* relating to our Personnel and *Personal Data* used in our business for our own commercial purposes.

Data Subject: a living, identified or identifiable individual about whom we hold *Personal Data*. *Data Subject*s may be nationals or residents of any country and may have legal rights regarding their *Personal Data*.

DPA: the Data Protection Act 2018.

Data Protection Legislation: the DPA and all other applicable data protection and privacy legislation in force from time to time in the UK.

***Data Protection Officer* (DPO)**: the person required to be appointed in specific circumstances under the *GDPR*.

Explicit Consent: *Consent* which requires a very clear and specific statement (that is, not just action).

Legitimate Interest: the interest of the firm in conducting and managing its business to enable it to give *Clients* the best service and the best and most secure experience. We make sure we consider and balance any potential impact on data subjects (both positive and negative) and their rights before we *Process* their personal data for our *Legitimate Interest*s. We do not use their personal data for activities where our interests are overridden by the impact on them (unless we have their *Consent* or are otherwise required or permitted to by law).

Personal Data: any information identifying a *Data Subject* or information relating to a *Data Subject* that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. *Personal Data* includes *Sensitive Personal Data* and *Pseudonymised Personal Data* but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal Data Breach: any act or omission that compromises the security, confidentiality, integrity or availability of *Personal Data* or the physical, technical, administrative or organisational safeguards that

we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of your *Personal Data* is a *Personal Data Breach*.

Process or Processing: any activity that involves the use of *Personal Data*. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. *Processing* also includes transmitting or transferring *Personal Data* to third parties.

Pseudonymisation or ***Pseudonymise***: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.

Sensitive Personal Data **(now called *Special Categories of Data* in the *DPA*)**: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual orientation, biometric or genetic data, and *Personal Data* relating to criminal offences and convictions.

UK: the United Kingdom of Great Britain and Northern Ireland

SCHEDULE 2

CLIENTS - TYPES OF DATA, AND LEGAL JUSTIFICATION FOR HOW WE USE IT

In the table below, we use the following abbreviations:

Type of Data

1 = **Identity Data** such as first name, maiden name, last name, username or similar identifier, marital status, title, date of birth and gender.

2 = **Contact Data** such as billing address, delivery address, email address and telephone numbers.

3 = **Financial Data** such as bank account and payment card details.

4 = **Transaction Data** such as details about payments to and from the *Client*.

5 = **Technical Data** such as internet protocol (IP) address, login data, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform and other technology on the devices used to access TWM's website.

6 = **Profile Data** such as interests, preferences, feedback and survey responses.

7 = **Usage Data** such as information about how the user navigates TWM's website.

8 = **Marketing and Communications Data** such as preferences in receiving marketing from us and other communication preferences.

We also collect, use and share aggregated data such as statistical or demographic data for any purpose. Aggregated data may be derived from *Personal Data* but is not considered *Personal Data* in law as this data does not directly or indirectly reveal the *Data Subject's* identity. For example, we may aggregate Usage Data to calculate the percentage of users accessing a specific website feature. However, if we combine or connect Aggregated Data with any *Personal Data* so that it can directly or indirectly identify the *Data Subject*, we must treat the combined data as *Personal Data* which will be used in accordance with this Policy.

Legal justification for *Processing*

A = TWM needs to *Process* the data in order to perform the contract we are about to enter into or have entered into with the *Client*.

B = TWM needs to *Process* the data in order to comply with a legal or regulatory obligation.

C = TWM *Process*es the data because it is necessary for our *Legitimate Interest*s (or those of a third party) and the interests and fundamental rights of the *Data Subject* do not override those interests.

Purpose/Activity	**Type of data**	**Legal justification for *Processing* (including basis of *Legitimate Interest*)**
To register the *Data Subject* as a new *Client*	1, 2	A
To *Process* and comply with the *Data Subject's* instructions including: (e) Manage payments, fees and charges (f) Collect and recover money owed to TWM	1, 2, 4, 8	A , C (to recover debts due to us)
To manage our relationship with *the Data Subject* which will include: (g) Notifying the *Data Subject* about changes to our terms or privacy policy (b) Asking the *Data Subject* to leave a review or take a survey	1, 2, 6, 8	A, B, C (to keep our records updated and to study how *Clients* use our products/services)
To enable *Data Subject*s to participate in a prize draw, competition or complete a survey	1, 2, 6, 8	A, C (to study how *Clients* use our products/services, to develop them and grow our business)
To administer and protect our business and our website (including troubleshooting, data analysis, testing, system maintenance, support, reporting and hosting of data)	1, 2, 5	B, C (for running our business, provision of administration and IT services, network security, to prevent fraud and in the context of a business reorganisation or group restructuring exercise)
To deliver relevant website content and advertisements to our *Clients* and contacts and measure or understand the effectiveness of the advertising we serve to them	1, 2 5, 6, 7, 8	C (to study how *Clients* use our products/services, to develop them, to grow our business and to inform our marketing strategy)
To use data analytics to improve our website, products/services, marketing, *Client* relationships and experiences	5, 7	C (to define types of *Clients* for our products and services, to keep our website updated and relevant, to develop our business and to inform our marketing strategy)
To make suggestions and recommendations to *Data Subject*s about products or services that may be of interest to them	1, 2 ,5, 6,7	C (to develop our products/services and grow our business)

SCHEDULE 3

INFORMATION ASSETS HELD BY TWM AND RELEVANT RETENTION PERIODS

Information Asset	Retention Schedule	Grounds for *Processing* Personal Data Usually Relied upon
Deeds, wills and other original client documents	Indefinite	Consent of the *Data Subject*. Contractual necessity. Necessary for compliance with a legal obligation. Necessary to protect the vital interests of data subject or another. Necessary for legitimate interests of *Data Subject* or other. Necessary under employment law. Necessary for conduct of legal claims.
Client files (paper)	Files will be destroyed after 10 years, except for commercial / residential purchase files which are retained for 15 years. Wills and Deeds are retained indefinitely or until requested by client or their executor.	Consent of the *Data Subject*. Contractual necessity. Necessary for compliance with a legal obligation. Necessary to protect the vital interests of *Data Subject* or another. Necessary for legitimate interests of subject or other. Necessary under employment law. Necessary for conduct of legal claims.
Client files (electronic): emails, drafts etc.	VMs - 30 days. SQL databases - first back up of the month held for 2 years, GFS rotation to tape held on tape for first back up of the month indefinitely and email archive kept for 7 years. Tapes held in fire safe.	Ditto
Client identification and verification information (copies of passports, utility bills, driving licence etc) under money laundering regulations. Generally, information obtained from clients would include: full names; marital status; date of birth; gender; billing, delivery and email addresses; telephone numbers; financial data including bank account and payment card details; and transaction data (includes payments to and from *Data Subject)*	Legal minimum retention period is five years from the end of the client relationship. In practice kept 10 years to allow for fresh instructions, with consent of clients, obtained at time of instruction. Also retained for conflict checking and professional indemnity reasons.	Consent of the *Data Subject*. Contractual necessity. Necessary for compliance with a legal obligation.
Records of internal anti-money laundering notifications and Suspicious Activity Reports	Indefinite	Contractual necessity. Necessary for compliance with a legal obligation.
Database of present and former clients	VMs - 30 days. SQL databases - first back up of the month held for 2 years, GFS rotation to tape held on tape for first back up of the month indefinitely and email archive kept for 7 years. Tapes held in fire safe.	Consent of the *Data Subject*. Contractual necessity. Necessary for compliance with a legal obligation.
Claims and complaints files	Closed claims and complaints are retained indefinitely.	Consent of the D*ata Subject*. Contractual necessity. Necessary for compliance with a legal obligation. Necessary to protect the vital interests of *Data Subject* or another. Necessary for legitimate interests of *Data Subject* or other. Necessary for conduct of legal claims.

Information Asset	Retention Schedule	Grounds for *Processing* Personal Data Usually Relied upon
Financial records including time recording data, bank data, accounts, payroll, VAT, PAYE, accountant's reports.	10 years: Payroll records and bank details	As above.
Health and safety certificates.	3 years from date of last entry - Accident Books/Accident Reports/records/First Aid and Fire Warden certificates. Other Health & Safety Certificates – permanently.	As above.
Files and information held in respect of predecessor, merged and acquired practices	VMs - 30 days. SQL databases - first back up of the month held for 2 years, GFS rotation to tape held on tape for first back up of the month indefinitely and email archive kept for 7 years. Tapes held in fire safe.	As above.
Website - IP addresses	Email archive	These are website enquiry forms directed to relevant fee earner to action. We store cookie information to understand browsing patterns and history, and we use IP address to identify generic location information eg town. We do not have specific street address etc.
Telephone audio recordings	7 years	Consent of the D*ata Subject* where applicable.

SCHEDULE 4

RIGHTS OF DATA SUBJECTS

1. *Data Subjects* have the following rights with regard to the *Personal Data* we hold about them, namely the right:

   (a) where Schedule 2 indicates TWM is relying on *Consent* to *Process* a *Data Subject's Personal Data*, to withdraw *Consent* at any time. However, this will not affect the lawfulness of any *Processing* carried out before the *Data Subject* withdraws their *Consent* or any *Processing* TWM carries out where we are not reliant on the *Data Subject's Consent*;

   (b) to receive certain information about the *Data Controller's Processing* activities;

   (c) to request access to the *Personal Data* that TWM holds about the *Data Subject* in order to check that it is accurate and complete and that we are *Processing* it lawfully;

   (d) to object to our use of the *Data Subject's Personal Data* for marketing purposes;

   (e) to ask us to delete or remove any of the *Data Subject's Personal Data* held by us where:

   - there is no good reason for us to continue to *Process* it;
   - the *Data Subject* has successfully exercised their right to object to *Processing* (see below);
   - TWM may have *Processed* a *Data Subject's Personal Data* unlawfully or where we are required to erase a *Data Subject's Personal Data* in order to comply with the law. Note, however, that we may not always be able to comply with a *Data Subject's* request for erasure for specific legal reasons which will be notified to the *Data Subject*, if applicable, at the time of their request.

   (f) to ask us to correct any inaccurate or incomplete *Personal Data* held relating to the *Data Subject.* Note that we may need to verify the accuracy of the new *Personal Data* the *Data Subject* provides to us;

   (g) to ask us to suspend the *Processing* of a *Data Subject's Personal Data* where:

   - the *Data Subject* wants us to establish the *Personal Data's* accuracy;
   - our use of the *Personal Data* is unlawful but the *Data Subject* does not want us to erase it;

- the *Data Subject* needs us to hold the data which we would not otherwise wish to hold for our own purposes, because the *Data Subject* needs it to establish, exercise or defend legal claims; or

- the *Data Subject* has objected to our use of their *Personal Data* but we needs to verify whether we have overriding legitimate grounds to use it.

(h) to object to the *Processing* of the *Data Subject's Personal Data* where we are relying on a *Legitimate Interest* (or those of a third party) and there is something about the *Data Subject's* particular situation which they feel impacts unfairly on their fundamental rights and freedoms, though, in some cases, we may demonstrate that we have compelling legitimate grounds to *Process* that information which override such rights and freedoms;

(i) to request a copy of an agreement under which the *Data Subject's Personal Data* is transferred outside of the UK;

(j) to object to decisions based solely on *Automated Processing*;

(k) to prevent *Processing* that is likely to cause damage or distress to the *Data Subject* or anyone else;

(l) to be notified of a *Personal Data* breach which is likely to result in high risk to their rights and freedoms;

(m) to make a complaint to the ICO, the UK supervisory authority for data protection issues, at any time. We would, however, like the opportunity to deal with your concerns before you approach the ICO so please contact us in the first instance; and

(n) where the *Data Subject* has provided information to us in electronic form which we needed to perform a contract with the *Data Subject*, or where we are relying on the *Data Subject's Consent* for the right to *Process* the data, to ask for your *Personal Data* to be transferred to you or to a third party in a structured, commonly used, and machine-readable format.

2. If a *Data Subject* wishes to exercise any of the rights set out above, they should contact us by sending an email to our *DPO*, Jamie Berry by email or by writing to him at TWM Solicitors LLP, 65 Woodbridge Road, Guildford, Surrey GU1 4RD.

3. *Data Subjects* will not normally need to pay a fee to access their *Personal Data* (or to exercise any of the other rights). However, we reserve the right to charge a reasonable fee if such a request is clearly unfounded, repetitive or excessively onerous. Alternatively, we have the right to decline to comply with such requests in these circumstances.

4. We may need to request specific information from a *Data Subject* to help us confirm their identity and ensure the *Data Subject's* right to access their *Personal Data* (or to exercise any of their other rights). This is a security measure to ensure that *Personal Data* is not disclosed to any person who has no right to receive it. We may also contact the *Data Subject* to ask them for further information in relation to their request in order to assist us to respond appropriately.

5. We endeavour to respond to all such legitimate requests within one month. Occasionally it may take us longer than a month if the request is particularly complex or the *Data Subject* has made a number of requests. In this case, we will notify the *Data Subject* and keep them updated.