DATA PROTECTION PRIVACY NOTICE
CLIENTS AND PROSPECTIVE CLIENTS

1. Introduction

We have set out below the obligations of Caveat Solicitors (our firm) regarding data protection and your rights as our client (data subjects) in respect of your personal data under UK General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA 2018).

This policy sets out our firms obligations regarding the collection, processing, transfer, storage, and disposal of your personal data, it explains when and why we collect personal information about our clients, how we use it and how we keep it secure and your rights in relation to it.

The GDPR defines personal data as 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. We will always comply with the General Data Protection Regulation (GDPR) when dealing with your personal data. Further details on the GDPR can be found at the website for the Information Commissioner(www.ico.gov.uk). For the purposes of the GDPR, we will be the"controller" of all personal data we hold about you.

We may collect, use and store your personal data, as described in this Data Protection Policy and as described when we collect data from you.

We reserve the right to amend this Data Protection Policy from time to time without prior notice. Every client of Caveat Solicitors will however be notified accordingly when the policy has been amended (but amendments will not be made retrospectively).

2. Policy Scope

This Policy applies to all clients and staff of Caveat Solicitors. It also applies to any third parties or stakeholders that are associated with Caveat Solicitors.

This policy applies to all data that Caveat Solicitors holds in relation to identifiable individuals including the following:

(i) Names, addresses, telephone numbers and emails
(ii) Date of Birth
(iii) Gender
(iv) Marital status
(v) Nationality

(vi) Bank details
(vii) Any other information relating to our clients.

3. What are our Data Protection Obligations?

GDPR requires data protection (or privacy)"by design and by default" as a legal obligation.
To comply with this, Caveat Solicitors will put measures in place to show that we have integrated data protection into our processing activities. This includes:
• Implementing privacy by design when processing personal data and completing privacy impact assessments where processing presents a high risk to rights and freedoms of individuals.
• Integrating data protection into internal documents including this policy, any related policies and any privacy notices.
• Regularly training staff on data protection law, this policy, any related policies and any other data protection matters. We must maintain a record of training attendance by staff.
• Regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance.
We will also conduct a data protection impact assessment when implementing new processes or systems

4. The Data Protection Principles

The GDPR sets out the following principles with which any party handling personal data must comply. All personal data must be:

1. Processed lawfully, fairly, and in a transparent manner in relation to the data subject.

2. Collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

3. Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.

4. Accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased, or rectified without delay.

5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of the data subject.

6. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

5. Your Rights (as a Data Subject)

The GDPR sets out the following rights applicable to data subjects (please refer to the parts of this policy indicated for further details):

1. The right to be informed;
2. The right of access;
3. The right to rectification;
4. The right to erasure (also known as the 'right to be forgotten');
5. The right to restrict processing;
6. The right to data portability;
7. The right to object; and
8. Rights with respect to automated decision-making and profiling.

6.How we obtain personal data

We obtain personal information in different ways, including through:

- Direct contact – individuals may give us their personal information by corresponding with us by post, email or telephone or otherwise.
- Clients – our clients may give us personal information of to enable us to provide our services
- Third parties or publicly available sources – we may receive personal information of individuals from third parties (for example disclosure by the police or CPS in connection with a prosecution) in connection with the provision of services by us to our clients. We may also receive information from publicly available sources such as Companies House and HM Land Registry

7.How we use personal data

We use personal data in a variety of ways including:

- To provide our services to our clients
- To recruit employees of Caveat Solicitors
- To manage and supervise our employees and Directors
- To promote our services
- To meet our legal and regulatory obligations
- To meet our audit and insurance obligations

8. Protecting your personal data

We will ensure that where information is collected, processed and stored electronically, generally accepted standards of technology and operational security is used and implemented in order to protect personal data from loss, misuse, or unauthorised alteration or destruction.

We will ensure that every electronic device is password protected and that only authorised persons have access to the device and the password. Only strong passwords shall be used. Where there are more than one authorised persons with access to one electronic device, each person will have their own password.

Please note however that where you are transmitting information to us over the internet this can never be guaranteed to be 100% secure.

Personal data will not be stored on permanent basis on small portable devices like memory sticks or smart phones unless it is for data transmission purposes.

Use of paper storage of personal data will be minimised. Any paperwork containing personal data shall be stored in a secure place and access to such paperwork shall be restricted to authorised persons.

Our paper files shall be stored in secure and lockable cabinets. Closed files shall also be securely stored.

Any electronically stored data that is no longer needed shall be deleted from the device permanently. Similarly, papers containing personal data shall be shredded or destroyed securely when no longer needed.

We will notify you promptly in the event of any breach of your personal data which might expose you to serious risk.

9. Your Information and third parties

During our retainer with you we may share your information with the following entities:

1. Courts and tribunals
2. Barristers & barristers chambers
3. Experts required to advise or provide reports
4. Accountants
5. Opposing lawyers and representatives
6. Solicitors Regulation Authority
7. Law Society
8. Legal Ombudsman
9. Banks and lenders
10. Mediation and arbitration service providers
11. Government bodies
12. Auditors
13. IT support, infrastructure and system providers
14. Employees of the firm
15. Contractors to the firm working on your matter
16. Postal service providers including couriers
17. Insurers and their advisors
18. Land Registry

We will securely destroy all financial information once we have used it and no longer need it.

10.Your legal rights about your personal data we process

Individuals have the rights set out below. If you wish to exercise any of these rights, please contact our Data Protection Officer.

- Request access to their personal information, commonly known as a subject access request (SAR). This enables individuals to receive a copy of the personal data we hold about them and to check that we are lawfully processing it.

If you wish to make a SAR, you may do so in writing. SARs should be addressed to the Caveat Solicitors Data Protection Officer (DPO), Rehana Choudhry.

Responses to SARs shall normally be made within one month of receipt, however we may extend by up to two months if the SAR is complex and/or numerous requests are made. If such additional time is required, you shall be informed.

All SARs received shall be handled by the firm's Data Protection Officer.

Our firm does not charge a fee for the handling of normal SARs. However, we reserve the right to charge reasonable fees for additional copies of information that has already been supplied to you, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

- Request correction of the personal information that we hold about them. This enables individuals to have any incomplete or inaccurate information we hold, though we will need to verify the accuracy of the new information provided to us.
- Request erasure of their personal information. This enables individuals to ask us to delete or remove personal information where there is no good reason for us continuing to process it. Individuals also have the right to ask us to delete or remove their personal information where they have successfully exercised their right to object to processing (see below), where we may have processed their information unlawfully or where we are required to erase their personal information to comply with local law. Note, however, that we may not always be able to comply with a request of erasure for specific legal reasons which will be notified to the individual, if applicable, at the time of their request.
- Object to processing of personal information where we are relying on a legitimate interest (or that of a third party) and there is something about the individual's particular situation which makes her/him want to object to processing on this ground as she/he feels it impacts on her/his fundamental rights and freedoms. In some cases, we may demonstrate that we have compelling legitimate grounds to process the information which overrides those rights and freedoms. Individuals also have the right to object where we are processing their personal information for direct marketing purposes.
- Request restriction of processing of their personal information. This enables individuals to ask us to suspend the processing of their personal information in the following scenarios: (a) if the individual wants us to establish the information's accuracy; (b) where our use of the information is unlawful but an individual does not want us to erase it; (c) where the individual needs us to hold the information even if we no longer require it as she/he needs it to establish, exercise or defend legal claims; or (d) the individual has objected to our use of their information but we need to verify whether we have overriding legitimate grounds to use it
- Withdraw consent at any time where we are relying on consent to process the personal information. However, this will not affect the lawfulness of any processing carried out before consent is withdrawn.

11. How long do we keep your information?

We will hold your personal data on our systems for as long as you are our client and for as long afterwards as it is in the company's legitimate interest to do so or for as long as is necessary to comply with our legal obligations. We will review your personal data every year to establish whether

we are still entitled to process it. If we decide that we are not entitled to do so, we will stop processing your personal data except that we will retain your personal data in an archived form in order to be able to comply with future legal obligations e.g. compliance with SRA regulations, tax requirements and exemptions, and the establishment, exercise or defence of legal claims.

12. Data Breaches

A data breach is defined in the GDPR as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data. We will take all reasonable endeavours to ensure that there are no Personal Data Breaches.

Any suspected personal data breach must be reported immediately to the DPO, Rehana Choudhry in addition to any other internal reporting requirements for regulatory compliance. In the unlikely event of a personal data breach, we will report this to the ICO within 72 hours of becoming aware of it, where the individual is likely to suffer some form of damage e.g. through identity theft or a breach of confidentiality.

13. Complaints

Individuals have a right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues (www.ico.org.co.uk). We would, however, appreciate the opportunity to deal with any concerns before the ICO is approached so please contact our Data Protection Officer, using the contact details given above, in the first instance.