DATA PROTECTION POLICY

Gumersalls, The White House, 16 Waterloo Road, Epsom, Surrey, KT19 8AZ

Tel: 01372 721122

Email: solicitors@gumersalls.co.uk

Website: www.gumersalls.co.uk

Background

- This Data Protection Policy sets out how Gumersalls Solicitors of The White House, 16 Waterloo Road, Epsom, Surrey KT18 5TD handle the Personal Data of our customers, suppliers, employees, workers and other third parties.
- **Personal Data** is any information identifying someone or information relating to them that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. It includes Sensitive Personal Data (ie. information revealing racial or ethnic origin, political opinions, religious beliefs, sexual orientation etc) 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 (ie. name, email address, location or date of birth) or an opinion about that person's actions or behaviour.
- It applies to **all** Personal Data we process, regardless of the media on which that data is stored or whether it relates to past or present employees, workers, customers, clients or supplier contracts, shareholders, website users or any other person. It applies to **all** people in the firm.
- Gumersalls has notified its data processing activities to the Information Commissioner's Office under registration number: Z6926230.

Scope

- Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we all take seriously at all times. The firm is exposed to potential fines of up to EUR20 million (approximately £18 million) or 4% of total worldwide annual turnover, whichever is higher and depending on the breach, for failure to comply with the provisions of the 'GDPR' (the General Data Protection Regulation).
- All Partners (and Supervisors) are responsible for ensuring that all staff comply with this Policy and need to implement appropriate practices, processes, controls and training to ensure such compliance.

- The Information Compliance Officer is responsible for overseeing this Policy and as applicable, developing related policies and privacy guidelines. That post is held by Tom Edwards. Please contact him (or the Deputy, Laura Pawley, if he is not available) with any queries about this Policy or if you have any concerns that it is not being followed.

- Always contact the Information Compliance Officer (or Deputy) if:
  - You are unsure of the lawful basis which you are relying on to process Personal Data
  - You are unsure about retention periods for data being processed
  - If there has been (or you think there has been) a Personal Data Breach

Personal data protection principles

We adhere to principles relating to the processing of personal data set out in the GDPR which require Personal Data to be:

- Processed lawfully, fairly and in a transparent manner
- Collected only for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed
- Accurate and where necessary kept up to date
- Not kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed
- Processed in a manner that ensures that its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against loss, destruction or damage
- Not transferred to another country without appropriate safeguards being in place
- Made available to data subjects and data subjects allowed to exercise certain rights in relation to their Personal Data

We are responsible for and must be able to demonstrate compliance with the data protection principles listed above.

1. *Fairness and Transparency*

The GDPR allows processing for specific purposes, some of which are set out below:

- The data subject has given consent
- The processing is necessary for purpose of providing its professional services and the administration of its client relationships
- To meet our legal compliance obligations
- To protect the data subject's vital interests
- To pursue our legitimate for purposes where they are not overridden because the processing prejudices the interests or fundamental rights and freedoms of data subjects. The purposes for which we process Personal Data for legitimate reasons need to be set out in applicable Privacy Notices/Fair Processing Notices;
- Other GDPR processing grounds

We must provide Privacy Notices or Fair Processing Notices to data subjects which are concise, transparent and in clear and plain language so they are easy to understand. Such Notices must include who we are, how and why we will use, process, disclose, protect and retain the personal data.

2. <u>Lawful Processing</u>

We must only process personal data, including sensitive personal data, lawfully where it has a valid basis for the processing. Typically, we process personal data on the basis of:

- Processing is necessary for the performance of a contract (eg. engagement letter) to which the data subject (ie. the client) is party or in order to take steps at the request of the data subject prior to entering into a contract;
- Processing necessary for the legitimate interests pursued by a client or the firm, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject. This ground may apply to the processing of the personal data of any third party data subjects whose personal data are provided by the client;
- A legal obligation to which we are subject and where compliance with such obligation necessitates the processing of personal data by us;
- Data subject's consent, where such consent is procured from the client; and
- Other legal grounds

3. <u>Purpose Limitation</u>

- Personal Data must be collected only for specified, explicit and legitimate purposes.

4. *Data Minimisation*

- Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is collected.
- We can only collect and process data we require to fulfil our professional obligations.
- When data is no longer needed for specified purposes, it must be deleted.

5. *Data Accuracy*

- We must take reasonable steps to ensure that personal data is accurate, complete and current for both clients and staff.

6. *Individual Rights*

- We must allow individuals to exercise their rights in relation to their personal data including their rights of access, erasure, rectification, portability and objection.

7. *Storage Limitation*

- We must only keep personal data for as long as it is needed for the purpose for which it was collected or for a further permitted purpose.
- We will keep all records as long as required by applicable law or may be necessary having regard to custom, practice or the nature of the documents concerned.
- Please refer to our Office Manual for details of our File Retention Procedures.
- Some data must be retained in order to comply with certain other legal obligations which are subject to (ie. Anti Money Laundering obligations) which override our obligations under the GDPR.

8. *Data Security*

- We must use appropriate security measures to protect personal data, including where third parties are processing personal data on our behalf.

9. *Accountability*

- We must have adequate resources and controls in place to ensure and document GDPR compliance, including: appointing someone accountable for data privacy; having internal documents including policies and keeping them up to date; regularly training staff on the GDPR, this policy etc; regularly testing and updating the measures put in place.

- We have put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or any applicable regulator where we are legally required to do so.
- If a Personal Data Breach has occurred or is suspected, no attempt to investigate the matter should be made. The Information Compliance Officer (Tom Edwards) or Deputy (Laura Pawley) should be contacted immediately (or a another partner if they are unavailable).
- Preserve all evidence relating to the potential breach/suspected breach.

10. Transfer Limitation

- Personal Data may only be transferred outside of the EEA if one of the following conditions applies:
  - The EC has issued an appropriate decision
  - Appropriate safeguards are in place (ie. binding corporate rules).
  - The Data Subject has provided Explicit Consent to the proposed transfer having been informed of the potential risks
  - It is necessary for one of the other reasons set out in the GDPR (ie. reasons of public interest).

11. Data Subject's rights and requests

- Rights of Data Subjects include:
  - Withdraw Consent to processing at any time
  - Request access to their Personal Data we hold
  - Ask us to erase data if it is no longer required, subject to our compliance with other obligations (ie. Anti Money Laundering regulations).
  - Be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms.
  - We must verify the identity of anyone making a request for data

12. Record Keeping

- We must keep and maintain accurate records reflecting our processing including consents.
- Records should include the name and contact details of the firm, the Data Security Officer, descriptions of personal data types, policies etc.

13. Training and Audit

- All partners and staff must undergo the training set by the Information Compliance Officer or Deputy within the timescales specified.
- All partners and staff must regularly review their systems and processes to ensure that they comply with this Policy.

14. Privacy by Design and Data Protection Impact Assessment (DPIA)

- We must implement appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR (Privacy by Design)
- All partners and staff must assess what measures can be implemented on all programs, systems that process Personal Data by taking into account the state of the art, the cost, the nature and the risks involved.
- A Data Protection Impact Assessment ('DPIA') should be undertaken when implementing major system or business change programs. This must include the description of the processing; an assessment of the necessity; risk to individuals and risk mitigation measures in place.

15. Automated Processing

- This means 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 predict aspects concerning that person's performance at work, economic situation, health etc.
- Making a decision based on this is generally prohibited when the decision has a legal or similar significant effect on an individual unless:
  - a Data Subject has Explicitly consented;
  - the processing is authorised by law; or
  - the processing is necessary for the performance of or entering into a contract.
- If relying on Automated Processing, the Data Subject must be informed correctly.
- A DPIA must be carried out before any Automated Processing activities are undertaken.

16. Direct Marketing

- A data subject's prior consent is required for electronic direct marketing (ie. by email, text or automated calls).
- The right to object must be explicitly offered and promptly honoured if they do object.

17. Sharing Personal Data

- Generally we are not allowed to share Personal Data with third parties unless certain safeguards and contractual agreements have been put in place. Always check with the Information Compliance Officer (or Deputy) if you are not sure if you can do so.

18. Changes to this Policy

- We reserve the right to change this Policy at any time without notice to you so please check back regularly to obtain the latest version.
- This Policy does not override any applicable national data privacy laws and regulations.

……..