KITTY ST AUBYN DATA PROTECTION POLICY

Contact details: kitty.staubyn@3rblaw.com

1. Introduction

1.1. The protection of personal data and respect for individual privacy is fundamental to the day-to-day operations of my practice.

1.2. This policy aims to protect and promote the data protection rights of individuals and of my practice, by setting out my data protection obligations and the procedures that must be followed in order to ensure compliance with the General Data Protection Regulation (GDPR) and the Data Protection Act 1998 (DPA).

1.3. This policy covers all personal data and special categories of personal data, processed on computers or stored in manual (paper based) files.

2. Responsibility

2.1. I am responsible for drafting and from time to time amending this policy and for its implementation.

2.2. I am responsible for monitoring compliance with this policy and I am the central point of contact for data protection issues relating to my practice (in particular, the handling of subject access requests pursuant to Article 15 GDPR).

2.3. I will cooperate, on request, with the Information Commissioner's Office in the performance of the latter's tasks.

3. The General Data Protection Regulation

3.1. The GDPR is designed to protect individuals and personal data which is held and processed about them by Chambers or other individuals.

3.2. The GDPR uses some key terms to refer to individuals, those processing personal data about individuals and types of data covered by the Regulation. These key terms are:

Personal data	Means any information relating to an identified and identifiable natural person ('data subject'). This includes for example information from which a person can be identified, directly or indirectly, by reference to an identifier i.e. name; ID number; location data; online identifiers etc. It also includes information that identified the physical, physiological, genetic, mental, economic, cultural or social identity of a person. For the purposes of my practice, my individual clients are data subjects (other individual third parties concerning whom I hold personal data about are also likely to be data subjects).
Controller	Means the natural or legal person, public authority, agency or other body who alone or jointly with others, determines the purposes and means of processing the personal data. In effect, this means the controller is the individual, organisation or other body that decides how personal data will be collected and used. For the purposes of my practice, I am a data controller for most of the personal data I process (see below for the limited circumstances in which I am a processor on behalf of another controller).
Processing	Means any operation which is performed on personal 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. For the purposes of my practice, everything that I do with client information (and personal information of third parties) is 'processing' as defined by the GDPR.
Processor	Means any natural or legal person, public authority, agency or other body that carries out any processing of personal data on behalf of a controller. From time to time I will act as a processor on behalf of Chambers, for example when working on

	Chambers committees or sub-committees, conducting recruitment exercises or at general meetings of Chambers.
Special category personal data	Means personal data revealing: a) racial or ethnic origin; b) political opinions; c) religious or philosophical beliefs; d) trade-union membership; e) the processing of genetic data or biometric data for the purpose of uniquely identifying a natural person; f) data concerning health or data concerning a natural person's sex life or sexual orientation; (g) data concerning criminal convictions.

4. Data Protection Principles

4.1. The GDPR is based around **seven** principles which are the starting point to ensure compliance with the Regulation. I must adhere to these principles in the conduct of my practice. The principles require me to ensure that all personal data and special category personal data are:

4.1.1. Processed lawfully, fairly and in a transparent manner in relation to the subject ('**lawfulness**, **fairness** and **transparency**').

4.1.2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('**purpose limitation**').

4.1.3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('**data minimisation**').

4.1.4. Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('**accuracy**').

4.1.5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which personal data are processed ('**storage limitation**').

4.1.6. Processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage using appropriate technical or organisational measures ('**integrity and confidentiality**').

4.2. Additionally, I must be able to demonstrate its compliance with the six principles set out above ('**accountability**').

5. Processing personal data and special category personal data

5.1. When processing data as a data controller, I will only do so:

5.1.1. with the consent of the data subject;

5.1.2. where the processing is necessary for the performance of a contract to which the data subject is a party (or in order to take steps at the request of the data subject prior to entering into the contract);

5.1.3. where the processing is necessary for compliance with its legal obligations; or

5.1.4. where the processing is necessary for the purposes of the legitimate interests I pursue or by a third party (namely the provision of legal or related services, management of conflicts, complaints, training, staff administration), except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

5.2. I must:

5.2.1. have legitimate grounds for collecting and using the personal data;

5.2.2. not use the data in ways that have unjustified adverse effects on the individuals concerned;

5.2.3. be transparent about how I intend to use the data, and give individuals appropriate privacy notices when collecting their personal data;

5.2.4. handle people's personal data only in ways they would reasonably expect; and
5.2.5. make sure I do not do anything unlawful with the data.

5.3. I will ensure that I am aware of the difference between personal data and special category personal data and ensure that both types of data are processed in accordance with the GDPR.

5.4. When processing special category personal data, I will only do so are when:
5.4.1. I have explicit consent from the data subject;
5.4.2. the processing is necessary for the purposes of performing a legal contract with the data subject, most commonly provision of legal services;
5.4.3. the processing is necessary for the purposes of carrying out my obligations in respect of employment and social security and social protection law;
5.4.4. the processing is necessary to protect the vital interests of the data subject or another person;
5.4.5. the processing relates to personal data that has already been made public by the data subject; or
5.4.6. the processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.

6. Retention

6.1. I will process personal data:
6.1.1. as a data controller, only for so long as is necessary to provide legal services to my clients or to comply with legal and professional conduct obligations to which I am subject; and
6.1.2. as a data processor, only for so long as instructed by the data controller.

In light of the above, the period for data retention will usually be seven years from the last date upon which the personal data was current (e.g. when I last supplied legal services to the client in relation to the matter to which the personal data relates) or when the legal or professional obligation to retain the personal data expires. In cases involving child defendants, the data will be retained until the client reaches 25 years of age. In cases where custodial sentences longer than 7 years have been passed, records will be kept until the end of the sentence. Departure from this policy is permitted where the client consents in writing to the data being held for a longer period.

6.2. The personal data I processed either as data controller or data processor will be periodically reviewed in order to ensure compliance with 6.1 above.

6.3. Personal data which should no longer be retained will be destroyed or permanently deleted in a secure manner.

7. Rights of the data subject

7.1. The GDPR gives rights to individuals in respect of the personal data that any organisations hold about them. These rights include:
7.1.1. The right to be provided with information about how their personal data is processed.
7.1.2. The right to access the personal data that is being processed about them and to obtain a copy.
7.1.3. The right to rectification of any inaccurate personal data.
7.1.4. The right to erasure of personal data held about them (in certain circumstances).
7.1.5. The right to restriction on the use of personal data held about them (in certain circumstances).
7.1.6. The right to data portability (the right to receive data processed by automated means and have it transferred to another data controller).
7.1.7. The right to object to the processing of their personal data.

7.2. I will process personal data in accordance with the rights of data subjects.

8. Security of personal data

8.1. I will implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk of likelihood and severity of its processing to the rights and freedoms of data subjects.

8.2. Such measures will include:
8.2.1. secure storage of digital and manual personal data;

8.2.2. encryption of personal data;
8.2.3. password protection to all devices capable of accessing personal data;

9. Confidentiality and data sharing

9.1. I will only share personal data with the following individuals or organisations when permitted or obliged to do so in accordance with law:
9.1.1. courts and other tribunals to whom documents are presented;
9.1.2. lay and professional clients;
9.1.3. potential witnesses, in particular experts, and friends or family of the data subject;
9.1.4. solicitors, barristers, representatives, pupils, mini pupils and other legal representatives;
9.1.5. ombudsmen and regulatory authorities;
9.1.6. current, past or prospective employers;
9.1.7. education and examining bodies;
9.1.8. business associates, professional advisers and trade bodies.

9.2. I contract with those on whose behalf I act as a data processor that:
9.2.1. I will process data only on instructions from the data controller;
9.2.2. I have committed myself (through compliance with this Policy) to confidentiality;
9.2.3. I will take all measures required to ensure the security of my data processing;
9.2.4. I will not engage third party suppliers / providers to process personal data controlled by the data controller without the written authorisation of the data controller, save where the law provides otherwise (where such authorisation is in general form, I shall inform the data controller of any intended changes concerning the addition or replacement of other processors, thereby giving the data controller the opportunity to object to such changes);
9.2.5. I will only use third party suppliers / providers pursuant to a written contract which provides sufficient guarantees that the third party will implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of the GDPR and ensure the protection of the rights of the data subject;
9.2.6. I will assist the data controller by appropriate technical and organisational measures, insofar as is possible, for the fulfilment of the data controller's obligations to respond to requests for exercising of data subjects' rights under Chapter III of the GDPR;
9.2.7. I will assist the data controller to ensure its compliance with Articles 32 to 36 of the GDPR;
9.2.8. at the choice of the data controller, I will delete or return all personal data as soon as practicable after the processing comes to an end or as otherwise directed by the data controller; and
9.2.9. I will make available to the data controller all information necessary to demonstrate compliance with Article 28 of the GDPR and allow for and contribute to audits, including inspections, conducted by the data controller.

9.3. Where I engage another processor to carry out specific processing activities on behalf the data controller, the same obligations as set out at 8.2 above shall be imposed on that other processor by way of a contract or other legal act. Where that other processor fails to fulfil its data protection obligations, I remain fully liable to the data controller for the performance of that other processor's obligations.

10. Record keeping

10.1. When acting as a data processor, I will keep a record of:
10.1.1. the name and contact details of each data controller on whose behalf I act as a data processor;
10.1.2. the categories of processing carried out on behalf of each data controller (as identified in their individual data protection policies);
10.1.3. where applicable, any transfers of personal data to third countries or organisations; and
10.1.4. where possible, a general description of the technical and organisational security measures

11. Breaches

11.1. A data protection breach is defined as “a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed” and may include circumstances in which personal data is:

11.1.1. accessed without authority;

11.1.2. processed unlawfully;

11.1.3. lost;

11.1.4. destroyed; or

11.1.5. damaged.

11.2. Breaches will be reported to the Information Commissioner’s Office (ICO) without undue delay and, where feasible, not later than 72 hours after I have become aware of the breach, unless I am able to demonstrate that the personal data breach is unlikely to result in a risk to the rights and freedoms of data subjects.

11.3. I will maintain a record of the details of any data protection breaches, comprising of the facts relating to the personal data breach, its effects and the remedial action taken.

11.4. When I act as a data processor on behalf of a data controller, I will notify the data controller of any personal data breach without undue delay after becoming aware of it.

12. Complaints

12.1. Complaints relating to breaches of the GDPR and/ or complaints that an individual’s personal data is not being processed in line with the data protection principles should be sent to me (at the email address given above) without delay.