FIONA WILLIAMS, 6 PUMP COURT

DATA PROTECTION POLICY

Particulars

Policy approval date:	24 May 2018
Policy operation date:	24 May 2018
Next review date:	24 May 2019
Data Controller:	Fiona Williams
Registration Number:	Z2155506
'Chambers' means:	Chambers of Stephen Hockman QC, 6 Pump Court, Temple, London, EC4Y 7AR.

Data Controller

Fiona Williams is a Data Controller within the meaning of, and regulated by, the General Data Protection Regulation (GDPR), and the GDPR and this Policy determines what purposes personal information is held or will be used for by Fiona Williams. The Data Controller is also responsible for notifying the Information Commissioner of the data held or that is likely to be held, and the general purposes that this data will be used for.

Fiona Williams is registered with the Information Commissioner's Office as a Data Controller under the registration number above.

Overview

This Policy is a suite of documents, which together make up the Data Protection Policy of Fiona Williams.

This Data Protection Policy is made up of the following documents:

1. General Data Protection Policy
2. Mobile Working Policy

3. Data Retention and Disposal Policy

4. Subject Access Request Policy

5. Data Breach Checklist

6. Joint Controllers Data Sharing Agreement

7. Data Controller and Data Processor Agreement

8. Privacy Notice

This Policy is publicly published on the Chambers website under Fiona Williams' profile and is accordingly constructively brought to the attention of all clients, potential clients, sources of instruction (whether solicitors, public bodies or via direct access), other members of the Bar, staff, employees, regulatory bodies such as the BSB or ICO, third-party contractors and service providers, and any other person with whom Fiona Williams deals as a barrister.

This Policy will govern all aspects of Fiona Williams' practice and activities as a Data Controller.

The Joint Controllers Data Sharing Agreement and Data Controller and Data Processor Agreement making up part of this Policy will be binding upon any person, organisation or body with whom Fiona Williams engages with respectively as a Joint Data Controller with Fiona Williams or as a Data Processor instructed or contracted by Fiona Williams.

Fiona Williams also adheres to 6 Pump Court's Data Protection, Privacy and Information Management Policy, which is publicly available on Chambers' website.

Definitions

Personal data	Any factual information or expressions of opinion relating to an individual where that individual can be identified directly from that information or in conjunction with any other information coming into the possession of the data holder.
Data Controller	The individual or organisation controlling personal data that decides the purpose of processing personal information, including what information will be processed and how it will be obtained.

Data Processor	An individual (other than an employee of the Data Controller) or organisation that processes personal information whilst undertaking a business activity or contracted service on behalf of the Data Controller.
Data processing	Any business activity or contracted service that involves using personal, corporate or other information for any purpose, including obtaining, recording, holding, viewing, storing, adapting, altering, deleting, disclosing. This is not restricted to computer processing but includes manual files and verbal discussions.

GENERAL DATA PROTECTION POLICY

Introduction

Fiona Williams needs to gather and use certain information about individuals.

These can include clients, customers, suppliers, business contacts, employees and other people the practice has a relationship with or may need to contact.

This Policy describes how this personal data must be collected, handled, stored to meet the practice's data protection standards – and to comply with the law.

Why this Policy Exists

This General Data Protection Policy exists to ensure that Fiona Williams:

- Complies with GDPR and follows good practice
- Protects the rights of staff, clients, customers and partners
- Is open about how individuals' data is stored and processed
- Is protected from the risks of a data breach

This Policy applies the provisions of the GDPR to Fiona Williams' practice and ensures compliance with the same.

Data Protection Law

The GDPR describes how organisations must collect, handle, and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The GDPR is underpinned by six important principles. They say that personal data must be:

1. Processed lawfully, fairly, and transparently
2. Collected for specific, explicit, and legitimate purposes
3. Adequate, relevant, and limited to what is necessary for processing
4. Accurate and, where necessary, kept up to date.
5. Kept in a form such that the Data Subject can be identified only as long as is necessary for processing
6. Processed in a manner that ensures appropriate security of the personal data

This Policy will be updated as necessary to reflect best practice in data management, security, and control and to ensure compliance with any changes or amendments made to the GDPR.

People, Risks and Responsibilities

People

This Policy applies to:

- Fiona Williams
- All employees or staff of Fiona Williams or Chambers, including volunteers, work experience students or support staff
- All contractors, suppliers and other people working on behalf of Fiona Williams

It applies to all data Fiona Williams holds relating to identifiable individuals. This can include but is not limited to names of individuals, postal addresses, email addresses, telephone

numbers, financial data, business names, plus any other personal sensitive information relating to individuals.

Risks

If personal data is not processed in accordance with this Policy and the GDPR generally, there is a risk of sanction against Fiona Williams by way of ICO penalty, prosecution or reputational damage, or of loss occasioned by compensation, damages and costs payable under a civil claim or complaint by a data subject.

Responsibilities

Fiona Williams and everyone who works for Fiona Williams either directly or indirectly has responsibility for ensuring data is collected, stored and handled appropriately.

This Policy will be updated as necessary to reflect best practice in data management, security, and control and to ensure compliance with any changes or amendments made to the GDPR.

General Data Protection Policy Information

Fiona Williams will, through appropriate management and strict application of criteria and controls:

- Observe fully conditions regarding the fair collection and use of information
- Meet its legal obligations to specify the purposes for which information is used
- Collect and process appropriate information, and only to the extent that it is needed to fulfil its operational needs or to comply with any legal requirements
- Ensure the quality of information used
- Ensure appropriate retention and disposal of information
- Ensure that the rights of people about whom information is held, can be fully exercised under the GDPR. These include:

- The right to be informed
- The right of access
- The right to rectification
- The right to erase
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

- Take appropriate technical and organisational security measures to safeguard personal information
- Ensure that personal information is not transferred outside the EEA without suitable safeguards
- Treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information
- Set out clear procedures for responding to requests for information

Data Storage

Information and records relating to service users will be stored securely and will only be accessible to authorised staff and Data Processors.

Information will be stored for only as long as it is needed or required statute and will be disposed of appropriately.

Fiona Williams will ensure all personal and company data is non-recoverable from any computer system when that system comes to be disposed of.

Data Access and Accuracy

All data subjects have the right to access the information Fiona Williams holds about them, except where specific exemptions apply to a legal professional. Fiona Williams will also take reasonable steps ensure that this information is kept up to date.

In addition, Fiona Williams will ensure that:

- Everyone processing personal information understands that they are contractually responsible for following good data protection practice
- Everyone processing personal information is appropriately trained to do so
- Everyone processing personal information is appropriately supervised
- Anybody interested in making enquiries about handling personal information knows what to do
- Enquiries about handling personal information are dealt with promptly and courteously
- The manner in which personal information is handled is explained clearly
- There will be a regular review and audit of the ways personal information is held, managed and used
- There will be a regular assessment and evaluation of the methods and performance in relation to handling personal information
- All Chambers staff are aware that a breach of the rules and procedures identified in this Policy may lead to disciplinary action being taken against them

Disclosure

Fiona Williams may share data with agencies such as government departments and other relevant parties.

The data subject will be made aware in most circumstances how and with whom their information will be shared. There are circumstances where the law allows Fiona Williams to disclose data (including sensitive data) without the data subject's consent.

These are:

- Carrying out a legal duty or as authorised by an appropriate government body
- Protecting vital interests of a data subject or other person
- The data subject has already made the information public
- Conducting any legal proceedings, obtaining legal advice or defending any legal rights
- Monitoring for equal opportunities purposes – i.e. race, disability or religion
- Providing a confidential service where the data subject's consent cannot be obtained or where it is reasonable to proceed without consent: e.g. where Fiona Williams would wish to avoid forcing stressed or ill data subjects to provide consent signatures.

Data Protection Training

Fiona Williams will ensure that any employees that work on data controlled by Fiona Williams are trained in data protection obligations and particularly this Policy annually.

If new members of staff commence work they will be provided with data protection training within the first month of employment.

Fiona Williams keeps a register of all training provided to staff.

Non-Conformance

Fiona Williams will self-report any data breaches to the ICO in accordance with the Data Breach Checklist below.

Any employee, staff member or worker of Fiona Williams or of Chambers found to have violated this Policy may be subject to disciplinary action, up to and including termination of employment.

Any third-party Data Processor which processes data controlled by Fiona Williams which fails to conform to the obligations under the GDPR will have action taken against it, either to terminate, suspend or reconsider such an instruction.

In case of any queries or questions in relation to this Policy please contact Fiona Williams via Chambers.

Practical Information on Data Processing

Fiona Williams processes personal data and sensitive personal data as follows:

1. Personal data is usually received either by hard copy or electronically. Hard copy personal data is usually received in Chambers where it is stored securely in the Clerks Room or equivalent until collected in person by Fiona Williams. Electronic personal data will usually be received by email, on removable storage media such as rewritable disks, or by download link. Such personal data will sometimes be processed by Chambers' clerks on behalf of Fiona Williams by first receiving the personal data to be forwarded on to Fiona Williams.

2. Personal data making up contact details and emails will be stored on Chambers' case management system and on email systems and on devices operated by Chambers' clerks as well as on Fiona Williams' systems, in order that data subjects can be contacted by both Fiona Williams, Chambers' clerks and by other members of Chambers when instructed on a case or if a case needs to be returned inside or outside of Chambers, and for Chambers to process Fiona Williams' fee invoices.

3. When hard copy papers are passed to Fiona Williams they will then be stored securely in Chambers, or taken out of Chambers for the purpose of Court hearings or to be worked on remotely in accordance with Fiona Williams' Mobile Working Policy.

4. When electronic documents or files are passed to Fiona Williams they will be saved onto Fiona Williams's work system, locally on a desktop computer, a laptop, a tablet

computer and a smartphone.

5. Electronic documents which are processed by Chambers' clerks as well as being passed to Fiona Williams by being attached to email will be saved to Chambers' case management system by the clerks and held securely by Chambers as a Data Processor for Fiona Williams.

6. When a case is complete the hard copy papers will be returned to the professional client if there is one. Papers relating to a direct access client's case will be retained unless requested otherwise.

7. When a case is complete the electronic file storing all data relating to that case will be marked accordingly, and will be reviewed under Fiona Williams's Data Retention and Disposal Policy.

8. Personal data may be shared with third parties, including third-party Data Processors, such as witnesses, experts, other members of Chambers, employees of Chambers (such as Clerks), judges or other decision-makers or tribunals, or recipients of marketing materials, but only ever for Fiona Williams' legitimate interests as a barrister. Fiona Williams will at all times adhere to the BSB Code of Conduct on client confidentiality.

MOBILE WORKING POLICY

Introduction

This Policy applies to Fiona Williams and any Data Processor instructed on Fiona Williams' practice who may remove case files, papers or other personal data from the precincts of Chambers' offices for the purposes of work.

Hard Copy Materials

Fiona Williams will adhere to the following rules on paper and other hard copy materials:

1. Fiona Williams will not remove client files or data from Chambers for any other reason than carrying out legitimate processing activities.

2. All files or case papers leaving Chambers are to be stored in an appropriately secured bag or box which remains under the control of the responsible person at all times.

3. Case files or papers will never be left freely available in any common area where they may be read by other individuals, e.g. unattended in court, in advocates' rooms in courthouses, in coffee shops, or at home.

4. Case files will not be left in a position where another person entering the room or looking through a window might inadvertently read them.

5. Case files will never be read or worked on in public where they can be overlooked by members of the public, including working on phones or laptops.

6. Case files may be worked on at home provided that the material is put away in a non-portable container when not in use. There will be appropriate physical security measures in place any files are stored for example, the use of burglar alarms and / or a lock on the room the files are in.

7. All case files will be moved securely. On public transport case files will not be left unattended. If travelling by private car, where practicable, they will be kept out of sight

and stored as inconspicuously as possible. Case files should not be left in a car unattended except where the risk is less of a risk than them being taken away. Case files should never be left in a car overnight.

8. Fiona Williams will not dispose of hard copy papers that contain any client data outside of Chambers, including handwritten notes, post-its etc. All hard copy paper disposals will take place in Chambers to meet confidential waste standards by secure shredding.

9. When no longer needed for the purpose of work off the premises of Chambers, all hard copy papers will be returned to Chambers as quickly as reasonably possible.

Electronic Devices

Fiona Williams will adhere to the following rules when processing personal data on electronic devices:

1. When accessing emails from a smartphone or tablet, the device will be suitably password-protected and, if appropriate, encrypted. Fiona Williams operates an 'inbox zero' policy so that the number of emails stored on any device are at a minimum.

2. Computers or devices will not be placed so that their screens can be overlooked, especially when working in co-working areas or public places.

3. Extreme care will be taken to ensure that client data and personal data relating to data subjects contained on laptops, removable devices and removable storage media is not lost or stolen.

4. Laptops and other removable devices will never be left unattended in public places or left in a car overnight

5. The material on any laptop or other removable device will be kept to the minimum necessary to enable work to be carried out efficiently

6. The electronic storage of case files will carry with it minimum levels of security, namely that all devices containing work-related data (whether or not this data amounts to personal data under the GDPR) will:

a) Be password-protected

b) Have up-to-date anti-virus and anti-spyware software

c) Be subjected to regular virus scans

d) Be protected by an appropriate firewall for the computer used

e) Only connect to secure wifi or mobile data internet connections, or public wifi connections via a virtual private network if appropriate

f) Have regular operating software updates

g) Have care taken with them such that malware or virus infection shall be avoided at all costs

h) Work in progress will be regularly backed up, and back-up media used for case files will be locked away securely, or be saved to a secure cloud computing folder

i) Computers used for working on case files at home will be protected from unauthorised and unrestricted access by third parties including family members.

7. The use of removable storage media (such as memory sticks, rewritable disks, removable hard disk drives and USB drives) will only be used to store personal data controlled by Fiona Williams with the express authorisation of Fiona Williams, and only in particular circumstances necessary for work-related purposes. Where Chambers receives removable storage media carrying data controlled by Fiona Williams from clients or third parties it will hold these securely until collected by Fiona Williams and such removable media will only be transferred in physical form by tracked or registered services such as tracked DX or post.

8. Laptop computers will be encrypted to FIPS 140-2 or CCTM (CESG Claims Tested Mark) standards or to such other standards as may be approved by Fiona Williams' professional clients. Whole-disk encryption rather than folder encryption is required.

9. Fiona Williams maintains a log of all computers and devices used for storing or working on case files. The log is maintained and updated from time to time and records type,

model and serial number of each device, together with the details and currency of any anti-virus, anti-spyware, encryption or other security software maintained on each machine. Fiona Williams will only use devices that are on this log for processing client data.

DATA RETENTION & DISPOSAL POLICY

Introduction

In the course of carrying out various functions, Fiona Williams creates and holds a wide range of recorded information. Records will be properly retained to enable Fiona Williams to meet the business needs of work at the self-employed regulated Bar, legal requirements imposed on Fiona Williams by the professional regulator or under other legislation, to evidence events or agreements in the event of allegations or disputes and to ensure that any records of historic value are preserved.

The untimely destruction of records could affect:

1. The conduct of Fiona Williams' business

2. The ability of Fiona Williams to defend or instigate legal actions

3. Fiona Williams' ability to comply with statutory obligations

4. Fiona Williams' reputation

Conversely, the permanent retention of records is undesirable and disposal is necessary to free up storage space, reduce administrative burden and to ensure that Fiona Williams does not unlawfully retain records for longer than necessary (particularly those containing personal data).

Purpose

The purpose of this Policy is to set out the length of time that Fiona Williams' records will be retained and the processes to review the records as to any further retention or for disposing of records at the end of the retention period.

Fiona Williams demonstrates accountability to proper data retention through the retention of records and by demonstrating that disposal decisions are taken with authority and in accordance with due process.

The Policy helps to ensure that Fiona Williams operates in compliance with the GDPR and any other legislative or regulatory retention obligations.

Scope

This Policy covers all data, information and records processed by Fiona Williams as a Data Controller wherever created or held and on whatever media, including: on paper; in electronic files (including databases, word processing documents, power point presentations, spreadsheets, webpages, PDF files, and e-mails); and photographs, scanned images, DVD-ROMs and videos.

This Policy covers all data, information and records processed by Fiona Williams as a Data Controller wherever created or held and such records may include, but are not limited to: client files; minutes of meetings; submissions from external parties; contracts and invoices; registers; legal advice; file notes; financial accounts; employee information; and publications.

Application

The Policy applies equally to Fiona Williams as a Data Controller and whoever or whatever may act as a Data Processor for Fiona Williams including Chambers, employees on a substantive or temporary contract, service providers, contractors, and any and all associated persons who work for Fiona Williams.

Minimum Retention Period

Unless a record has been marked for ‘permanent preservation’ Fiona Williams’ policy will be to only be retain data for a period of 9 years. This minimum retention period has been formulated on the basis that this allows a client or third party to issue proceedings or a complaint against Fiona Williams within then applicable limitation period of six years, plus a period of three years to allow for appeals or the active period of a case to elapse before limitation starts to run.

The minimum retention period has been calculated taking account of:

1. The business need of Fiona Williams’ practice

2. Applicable legislation

3. The need for Fiona Williams to respond to complaints

4. The ability of Fiona Williams to take or defend legal action.

Disposal

What is Disposal?

Fiona Williams is responsible for ensuring that all data held is periodically reviewed at least annually to determine whether any retention periods have expired. This will take the form of assessing the 'Last Modified' or 'Date Saved' metadata for electronic files, the noted 'Case Closed' date on paper files, or the 'Date Sent' metadata for emails. Once the retention period has expired, the data will be reviewed and a 'disposal action' agreed upon.

A 'disposal action' is;

1. The destruction of the record
2. The retention of the record for a specific further period in order to facilitate Fiona Williams' practice, or
3. Alternative disposal of the record e.g. returning papers to the instructing solicitor

Making and Recording the Disposal Decision

A review of the data will take place as soon as possible after the expiry of the retention period or, if that is not feasible, the data will be retained and a later review date set. This may not be a detailed or time-consuming exercise but there will be a considered appraisal of the contents of the data. The review will be conducted by the Fiona Williams.

The disposal decision will be reached having regard to:

- The on-going business and accountability needs of Fiona Williams' practice
- Applicable legislation
- Whether the record has any long-term historical or research value
- The best practice in the legal industry

- Any costs associated with continued storage versus costs of destruction;
- The legal, political and reputational risks associated with keeping, destroying or losing control over the record.

Destruction

No destruction of data will take place without assurance that:

- The data is no longer required by any part of Fiona Williams' practice
- No work is outstanding on any instructions on the case in question or any related case
- No litigation or investigation is current or pending which affects the data
- There are no current or pending FOIA or GDPR subject access requests which affect the record.

Destruction of Paper Records

Destruction will be carried out in a way that preserves the confidentiality of the data. Non-confidential records may be placed in ordinary rubbish bins or recycling bins. Confidential records will always be placed in confidential waste bins or shredded and placed in paper rubbish sacks for collection by an approved disposal firm. All copies, including security copies, preservation copies and backup copies will be destroyed at the same time in the same manner.

Destruction of Electronic Records

All electronic records will be either physically destroyed or wiped. Deletion of the files simply by over-writing will not be sufficient, save that the data may be deleted pending the eventual physical destruction or wiping of the device in question.

Further Retention

Upon review the data may be retained for a further period if it has on-going business value or if there is specific legislation which requires it to be held for a further period.

SUBJECT ACCESS REQUEST POLICY

Subject Access Requests

All individuals who are the subject of personal data held by Fiona Williams are entitled to:

1. Ask what information Fiona Williams holds about them and why
2. Ask how to gain access to it
3. Be informed how to keep it up to date
4. Be informed how the company is meeting its data protection obligations

If an individual contacts Fiona Williams requesting this information, this is called a subject access request. This request is to be dealt with promptly and in any event within one month. Fiona Williams can be contacted at the address at the top of this Policy.

Fiona Williams may carry out any of the following before releasing data further to a subject access request:

1. Request photographic proof of identification before sharing any information.
2. Check if there are any exemptions contained within the GDPR which prevent the sharing of this information with the data subject
3. Clarify and request further details about the subject access request if it is unclear before providing a copy of all information within one calendar month of receipt of a clear request.

DATA BREACH MANAGEMENT CHECKLIST

Introduction

This Policy will apply as a Checklist to guide Fiona Williams through the steps necessary upon any data breach or suspected data breach occurring in respect of data for which Fiona Williams is the Data Controller

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"*.

Fiona Williams will also follow the Chambers Data Protection Breach Reporting Procedure under the Chambers Data Protection, Privacy and Information Management Policy where appropriate.

Investigate

Record details of the data breach:

1. Describe the incident in as much detail as possible.
2. When did the incident happen?
3. How did the incident happen?
4. Has there been any delay between the breach happening and the breach being investigated?
5. What is the scope of the breach?
6. What data has been breached?
7. How many data subjects are affected?
8. Are any of the data subjects at risk as a result of the breach?
9. What type of information is involved? Is it commercial or personal?
10. What can happen to the information? How could it be used to a detrimental effect? What

action could be taken to deal with those effects?

11. If data has been lost or stolen, are there any safeguards in place such as encryption?

Containment

Record what technical systems have been affected:

7. Emails

8. Cloud or server storage

9. Case or practice management systems

10. Mobile devices

11. Home or Chambers internet access

What can you do to prevent further loss or consequences?

Notification

Consider who needs to be notified of the breach:

1. Instructing solicitors or department, or direct access client if appropriate

2. Individuals who are the subjects of the data

3. Chambers' Data Protection Officer

4. Head of Chambers

5. Chambers' Senior Clerk

6. Email and/or Chambers' case management systems service provider

7. Police

8. Bar Standards Board

9. Information Commissioner's Office

10. Professional indemnity insurer

11. CJSM

Sources of Assistance

Do you need to get legal advice?

Do you need PR assistance in relation to media attention?

Can your IT providers help?

Can Chambers assist?

Communications

Ensure that every person provided with information about the incident understands the need for confidentiality.

Ensure that there is a clear communication strategy with a central point of contact.

All communications relevant to the incident should be restricted to an agreed group of people to avoid any unintended waiver of privilege or other unplanned disclosure of information.

Evaluation

Assess why the breach occurred and review systems to prevent recurrence.

Prepare a report in writing for the ICO if the data breach is reportable.

JOINT CONTROLLERS DATA SHARING AGREEMENT

Between

Fiona Williams

Registered Data Controller Ref No. Z2155506

And

Any Data Controller instructing Fiona Williams to carry out regulated activities as a barrister

Dated

The date instructions are received

Introduction

1. The parties to this Agreement will work together to advise, provide expertise to or represent lay clients in legal proceedings. The exchange of information facilitates this partnership and should always adhere to legal requirements under the GDPR.

2. For the purposes of this Agreement the Parties jointly handle and process personal data and sensitive personal data as defined in the GDPR and are accordingly Joint Data Controllers within the meaning of the GDPR. This joint control is primarily applicable to the personal data of a lay client(s) where the instructing party is Fiona Williams' professional client.

Parties

3. This Joint Controllers Data Sharing Agreement ("Agreement") is between:

(1) Fiona Williams as a Data Controller

And

(2) Any Data Controller instructing Fiona Williams

(each “a Joint Party” and jointly “the Joint Parties”)

Supplemental Agreement

4. This Agreement is supplemental to any other separate contract entered into between the Joint Parties and exists to ensure that there are sufficient security guarantees in place for the safe sharing of personal data and sensitive personal data in accordance with the GDPR.

5. Information to which this Agreement relates must be handled in accordance with the appropriate legislative and regulatory environment and each Joint Party’s relevant policies and procedures.

Commencement of Agreement

6. This Agreement will commence immediately upon Fiona Williams receiving formal instructions from a Data Controller to carry out any task appropriate for a barrister and upon the transfer of any personal data to Fiona Williams, if transferred prior to formal instruction, and where Fiona Williams and the other Joint Party are Joint Data Controllers.

Length of Agreement

7. This Agreement will remain in place until terminated by either Joint Party and will apply to all cases for all clients that the Joint Parties work on together, now and in the future, unless expressly stated otherwise.

Definitions

8. For the purposes of this agreement “Relevant Information” shall mean any or all personal or sensitive personal data (as defined by the GDPR) relating to a client or clients or a case on which the Joint Parties are working together, or the personal or sensitive personal data of data subjects within that client or clients, or connected with the case in question in any fashion.

Purpose and Objectives of the Data Sharing

9. The purpose of the sharing of data detailed in this Agreement is to provide legal advice and representation to the client or clients.

Transfer and Frequency of Data

10. Relevant Information will be shared as and when required for both Joint Parties to discharge their responsibilities to the client(s) and to provide representation in the case appropriately.

Access & Security

11. Under no circumstances should Relevant Information be left unattended or processed in any way that is unsecure.

12. Each Joint Party shall notify the others as soon as is practicable, and at a maximum within five working days, if they become aware of any unauthorised or unlawful processing, loss, damage or destruction of the Relevant Information. This includes any 'near misses' and any incidents reported to the ICO. It is the responsibility of the Joint Party managing the incidents to investigate, report and escalate them as appropriate to the necessary regulatory bodies.

13. Relevant Information will be shared on a strict need-to-know basis only and will only be processed by employees or third-party Data Processors of either Joint Party in order for them to perform their duties in accordance with one or more of the defined purposes.

14. Each Joint Party shall ensure that any processor, agent or subcontractor instructed by them to process Relevant Information will process such information in accordance with the GDPR, and that all appropriate data sharing or processing agreements or contracts are in place.

15. Each Party will ensure that all staff with access to the Relevant Information have received appropriate data protection or information governance training and are aware of the confidential nature and duties placed on those processing such information. This includes ensuring they have appropriate monitoring policies and procedures in place for all staff.

16. Failure to meet the standards within this Agreement will result in Relevant Information not being shared, which could result in the termination of this and other service agreements.

Processing of Relevant Information

17. Each Party remains responsible for the Relevant Information held and processed within their own systems.

18. Each Joint Party will ensure Relevant Information will not be processed outside of the European Economic Area without the appropriate safeguards being in place to satisfy the GDPR.

19. Each party will comply fully with the GDPR and other relevant legislation. Particular attention must be paid to Principle 6 and ensuring the security of Relevant Information and systems. Each Joint Party will protect such information from unauthorised or unlawful processing, accidental loss, destruction or damage, and acknowledge that they have implemented the required technical and organisational measures.

GDPR and the Freedom of Information Act 2000 Subject Access Requests

20. Each Party is responsible for complying with complaints, queries and objections regarding Relevant Information sharing, subject access and freedom of information requests directed to their respective organisation in line with the relevant legislation or policies in practice. Each individual request must be dealt with on a case by case basis and the consequences of their decisions (for example, to object to sharing) must be clearly explained to the individuals in writing by the party receiving the request.

21. Each Party shall inform the other of any data subject access requests made in respect data which is jointly controlled.

Retention periods

22. Relevant Information will be retained in line with each party's data retention policy, which both parties confirm meets the requirements under the GDPR.

Disposal of information

23. Both Parties are individually responsible for deleting or safely disposing of Relevant Information when it is no longer required in line with their own data protection policies, which both parties confirm meet the requirements of the GDPR.

Termination and Variation

24. Any Party may terminate this Agreement by giving one calendar month's notice in writing to the other Parties. The terms of this agreement remain binding on any information shared and retained throughout its lifecycle, irrespective of whether the party remains a current signatory to this agreement.

25. Any proposed changes to the Parties involved in this Agreement, to the purposes of the information sharing, the nature or type of information shared or manner in which the information is to be processed and any other suggested changes to the terms of this Agreement must be notified immediately to key contacts within each party so that the impact of the proposed changes can be assessed.

26. This Agreement shall be governed and construed in accordance with English Law and the parties agree to submit to the exclusive jurisdiction of the Courts of England and Wales.

DATA CONTROLLER AND DATA PROCESSOR AGREEMENT

Between

Fiona Williams

Registered Data Controller Ref No. Z2155506

And

Any Data Processor instructed or contracted by Fiona Williams to carry out any form of data processing

Dated

The date instructions are received, or a contract for services is formed

Introduction

1. Fiona Williams will instruct Data Processors to act to process personal data for which Fiona Williams is the applicable Data Controller.

2. Because the services require the processing of personal data and sensitive personal data, the GDPR is engaged. Fiona Williams remains the Data Controller and legally responsible for that data processing under the GDPR.

3. The 6th Principle of the GDPR requires a Data Controller, when using the services of another organisation or company to process personal data on their behalf (a Data Processor), to:

   a) Choose a Data Processor which can provide sufficient guarantees about their data security measures to protect the personal data they will be processing as part of the contract

   b) Take reasonable steps to make sure those security measures are in place and sustained

c) Document what the Data Processor is allowed to do with the personal data in a written contract. The contract must include: what they can and what they cannot do with the personal data; what security measures must be in place to protect the data; what procedures must be followed if there is a data breach; and any other arrangements i.e. sub-contracting, termination of contract etc. that needs to be included to secure and control the data, including the requirement for the Data Processor to comply with obligations equivalent to those imposed on the Data Controller by the 6th Principle.

d) Take steps to ensure that: the personal data remains protected; the liabilities and risks are appropriately managed; data is processed lawfully; and the contract is legally enforceable.

e) Not allow processing of personal data unless the processing is carried out under the written contract, and only when the Data Processor is instructed to process personal data by the Data Controller.

4. Fiona Williams as a Data Controller wishes to engage the services of the Provider as a Data Processor to process personal data which Fiona Williams controls as a Data Controller.

Parties

5. This Data Controller and Data Processor Agreement ("Agreement") is between:

(1) Fiona Williams as a Data Controller

And

(2) Any Data Processor (within the meaning of the GDPR) instructed or contracted by Fiona Williams to provide services where personal data controlled by Fiona Williams is processed ("the Provider")

(each “a Party” and jointly “the Parties”)

Supplemental Agreement

6. This Agreement is supplemental to any other separate contract entered into between the Parties (a “Main Contract”) and exists to ensure that there are sufficient security guarantees in place for the safe processing of personal data and sensitive personal data in accordance with the GDPR.

7. Information to which this Agreement relates must be handled in accordance with the appropriate legislative and regulatory environment and each Party’s relevant policies and procedures.

Commencement of Agreement

8. This Agreement will commence immediately upon Fiona Williams sending instructions to, or contracting with, the Provider to carry out any task involving the processing of personal data and upon the transfer of any personal data to such a Data Processor in any event.

Length of Agreement

9. This Agreement will remain in place until terminated by either Party or until the Provider ceases to process personal data for Fiona Williams under any Main Contract.

Data Controller Rights and Responsibilities

10. Fiona Williams is the Data Controller of the personal data and is responsible for ensuring it is processed fairly and lawfully and in accordance with the GDPR.

11. Under the GDPR, it is the legal duty of a Data Controller to ensure the data protection Principles are met when personal data he or she controls is processed, unless an exemption applies.

12. Fiona Williams remains legally responsible for the data processing carried out by the contracted Provider as Data Processor.

13. Fiona Williams shall not instruct the Provider to process personal data under this Agreement where there is not a secure basis in law for that data to be processed.

14. Fiona Williams, as the Data Controller, is entitled during the term of this Agreement to require the Provider to provide reasonable assurances that technical and organisational security measures adequately protect the personal data it is contracted to process.

Data Processor Responsibilities

15. As a Data Processor the Provider shall at all time process personal data only as instructed to do so by Fiona Williams as the Data Controller and in accordance with the GDPR and this Agreement.

16. The Provider shall have in place appropriate technical and organisational security measures that protect the personal data it is contracted to process on behalf of the Data Controller from unauthorised or unlawful processing, accidental loss, destruction or damage.

17. The Provider shall provide reasonable assurances and guarantees to Fiona Williams as required that those technical and organisational security measures in place are both appropriate and effective in protecting the processing of personal data.

18. The Provider agrees to maintain good information governance standards and practices, by meeting or exceeding the data protection requirements relevant for its services.

19. The Provider shall not share the personal data with any third party without the prior written permission of Fiona Williams or process personal data in any way or for any purpose that it has not been instructed and authorised by Fiona Williams, or sub-contract a third party to process Fiona Williams' personal data without the prior knowledge and written agreement of Fiona Williams, and only then having provided all the necessary assurance and guarantees of their adequate organisational and technical security measures.

20. The Provider shall not transfer or permit the transfer of the personal data on to any territory outside the European Economic Area without the prior knowledge and written agreement of Fiona Williams.

Data Security Requirements

21. The Provider shall:

a) Have regard to the state of technological development and to the cost of implementing any measures, provide a level of security (including appropriate technical and organisational measures) appropriate to the harm that might result from unauthorised or unlawful processing of personal data or the accidental loss, damage or destruction of personal data and the nature of that personal data.

b) Ensure that access to the personal data is limited to those employees who need access to meet the Provider's obligations under this Agreement.

c) Take reasonable steps to ensure the reliability of their personnel who have access to Fiona Williams' controlled personal data, which shall include ensuring that all staff engaged by the Provider: understand the confidential nature of the personal data; have received appropriate training in data protection prior to their use of the data; and have signed a written undertaking that they understand and will act in accordance with their responsibilities for confidentiality under contract.

d) Ensure that it has properly configured access rights for its staff, including a well-defined starters and leavers process to ensure appropriate access control.

e) Ensure that suitable and effective authentication processes are established and used to protect personal data.

f) Ensure that the personal data is backed up on a regular basis and that any back-up data is subject to vigorous security measures as necessary to protect the availability, integrity and confidentiality of the data

g) Implement robust and tested business continuity measures to protect the confidentiality, integrity and availability of Fiona Williams' controlled personal data.

h) Encrypt data transferred electronically in accordance with national standards.

i) Ensure that employees are not able to access data remotely, e.g. from home or via their own electronic device or internet portal, other than through a secure

electronic network and in accordance with an organisational remote working policy.

j) Only dispose of data securely and confidentially when it requires disposal.

Information Breach Incident Reporting

22. The Provider shall have procedures in place to monitor access and to identify unauthorised and unlawful access and use of personal data.

23. The Provider shall immediately report to Fiona Williams any information security incidents relating to a personal data subject whose personal data controlled by Fiona Williams and undertakes to also fully cooperate with Fiona Williams' incident investigation requirements.

24. It is Fiona Williams' responsibility as Data Controller to ensure that the incident is reported in accordance with the law and informing the relevant data subjects as appropriate.

Secure Destruction

25. The Provider shall ensure that personal data held in paper form (regardless of whether originally provided by Fiona Williams or printed from the Provider's systems) is destroyed using a cross cut shredder or subcontracted to a confidential waste company.

26. The Data Processor shall ensure that electronic storage media used to hold or to process personal data is destroyed or overwritten when no longer in use.

27. In the event of any bad or unusable sectors on electronic media that cannot be overwritten, the Provider shall ensure complete and irretrievable destruction of the media itself.

28. The Provider shall provide Fiona Williams with copies of all relevant overwriting verification reports and/or certificates of secure destruction of personal data at the conclusion of the contract, if requested.

Variations

29. Any variation to the terms of this contract shall be agreed in writing by the Parties and

in accordance with the contract management conditions set out in any Main Contract.

Dispute Resolution

30. The Parties shall aim to resolve all disputes, differences and questions by means of co-operation and consultation and in accordance with any dispute resolution process specified in the Main Contract.

Termination

31. Fiona Williams may terminate this Agreement with immediate effect by written notice to the Provider on or at any time after the occurrence of an event that gives rise to an information security incident or otherwise poses a risk of non-compliance with the data protection principles.

32. Upon this Agreement ending the Provider shall securely return any personal data held or make arrangements for its secure destruction upon being instructed to do so by Fiona Williams.

PRIVACY NOTICE

I will take all possible steps to protect your personal information. I am determined to do nothing that would infringe your rights or undermine your trust. This Privacy Notice describes the information I collect about you, how it is used and shared, and your rights regarding it.

Privacy Notice for Data Subjects under Article 13 GDPR

This Privacy Notice applies to data subjects who have sent me their personal data.

Privacy Notice for Data Subjects under Article 14 GDPR

This Privacy Notice applies to data subjects who have not sent me their personal data but where I have received that personal data via a third party.

Data Controller

I am registered with the ICO as a Data Controller for the personal data that I hold and process as a barrister. My registered address is Chambers of Stephen Hockman QC, 6 Pump Court, Temple, London, EC4Y 7AR and my ICO registration number is Z2155506.

Data Collection

All the information that I hold about you is provided to or gathered by me in the course of a case and/or proceedings and/or for another reason connected to my practice as a barrister. If you have instructed me via a solicitor, your solicitor and I are Joint Data Controllers and we will tell you why we need the information and how we will use it. If you have instructed me via direct access or have not instructed me to represent you, I will be the applicable Data Controller and I will tell you why I need the information and how I will use it

I collect and process both personal data and special categories of personal data as defined in the GDPR. This includes:

- Names
- Emails
- Phone numbers
- Addresses
- Payment or bank details
- Dates of birth
- Location details
- Financial information
- Medical Records
- Criminal Records

Lawful Basis for Processing

The GDPR requires all organisations that process personal data to have a Lawful Basis for

doing so. The Lawful Bases identified in the GDPR are:

- Consent of the data subject
- Performance of a contract with the data subject or to take steps to enter into a contract
- Compliance with a legal obligation
- To protect the vital interests of a data subject or another person
- Performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
- The legitimate interests of the data controller, or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject

Examples of legitimate interests include:

- Where the data subject is a client or in the service of the controller
- Transmission within a group of undertakings for internal administrative purposes
- Processing necessary to ensure network and information security, including preventing unauthorised access
- Processing for direct marketing purposes, or to prevent fraud
- Reporting possible criminal acts or threats to public security

The Lawful Basis on which I will process your data is that of my legitimate interests and my

legitimate interests are, variously as the case may be:

- That I need to process your personal data as you are my lay client and I cannot represent you without processing your personal data.
- That you are a potential client and I need to process your personal data to market to you or to engage with you with a view to you becoming my client.
- That you are part of an instructing body or professional client such as a firm of solicitors or instructing department, and I cannot be instructed by you without processing your personal data.
- That you are a member, employee, contractor, staff member, pupil or mini-pupil of Chambers, or a prospective member of any of those classes of person, and I need to process your personal data in order to facilitate that relationship.
- That you are an opponent on a case, an employee of the Courts or another tribunal, a witness, family member or friend or other contact of my client, a judge or other decision maker, a member of a regulatory body such as the BSB, a member of the Bar Council, or any other third party of any other description whose personal data I will process for any reason howsoever connected to my practice, and in each case I will need to process your personal data in order to operate as a barrister.

Use

I use your information to:

- Provide legal advice and representation
- Assist in training pupils and mini-pupils
- Investigate and address your concerns

- Communicate with you about news, updates and events
- Investigate or address legal proceedings relating to your use of my services/products, or as otherwise allowed by applicable law
- Make statutory returns as required by HMRC, the BSB or any other body

I do not use automated decision-making in the processing of your personal data.

Sharing

I may share your personal data with:

- Instructing solicitors or departments
- Pupils or mini-pupils under my training or under the training of other members of Chambers
- Other members of my Chambers
- Opposing counsel
- My Chambers management and staff who provide administrative services such as clerks
- The Bar Standards Board or other regulatory body or legal advisors in the event of a dispute or other legal matter
- Law enforcement officials, government authorities, or other third parties to meet my legal obligations
- Publicly by way of marketing or advertisement where your case has been published in a law report or otherwise

- Judicial appointment bodies or legal rankings services

- Service providers carrying out services for me, such as ICT or internet service providers

Retention

I retain your personal data while you remain a data subject whose data I have a legitimate interest in processing, unless you ask me to delete it. My Retention and Disposal Policy (see above) details how long I hold data for and how I dispose of it when it no longer needs to be held. I will delete or anonymise your information at your request unless:

- There is an unresolved issue, such as claim or dispute
- I am legally required to, or
- There are overriding legitimate interests, including but not limited to fraud prevention and protecting customers' safety and security.

Your Rights

The GDPR gives you specific rights around your personal data. For example, you have to be informed about the information I hold and what I use it for, you can ask for a copy of the personal information I hold about you, you can ask me to correct any inaccuracies with the personal data I hold, you can ask me to stop sending you direct mail, or emails, or in some circumstances ask me to stop processing your details. Finally, if I do something irregular or improper with your personal data you can seek compensation for any distress you are caused or loss you have incurred. You can find out more information from the ICO’s website and this

is the organisation that you can complain to if you are unhappy with how I dealt with you.

Accessing and Correcting Personal Data

You may request access to, correction of, or a copy of your information by contacting me via Chambers.

Updates

I will occasionally update my Privacy Notice. When I make significant changes, I will publish the updated Notice on my website profile.