Pascal Bates, 6 PUMP COURT

DATA PROTECTION POLICY

Particulars

Policy approval date:	7 June 2018
Policy operation date:	7 June 2018
Next review date:	1 June 2019
Data Controller:	Pascal Bates
Registration Number:	Z6394031

Data Controller

Pascal Bates 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 Pascal Bates. The Data Controller is also responsible for notifying the Information Commissioner's Office of the data held or that is likely to be held, and the general purposes that this data will be used for.

Pascal Bates 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 Pascal Bates.

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 Pascal Bates’ 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 Pascal Bates deals as a barrister.

This Policy will govern all aspects of Pascal Bates’ 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 Pascal Bates engages with respectively as a Joint Data Controller with Pascal Bates or as a Data Processor instructed or contracted by Pascal Bates.

Pascal Bates also adheres to Chambers’ Data Protection, Privacy and Information Management Policy, which is publicly available on Chambers’ website, though in the event of any perceived conflict, the provisions of this policy shall take precedence over that of any Chambers policy.

Definitions

BSB Bar Standards Board.

Chambers The barristers’ chambers known as the “Chambers of Stephen Hockman QC” and/or as “6 Pump Court” and primarily situated at 6 Pump Court, Temple, London, EC4Y 7AR.

Data Controller An individual or organisation controlling Personal Data who decides the purpose of processing personal information, including what information will be processed and how it will be obtained.

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.

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 Subject

An individual whose Personal Data is the subject of Data Processing by the Data Controller or any Data Processor acting for the Data Controller.

GDPR

General Data Protection Regulation.

ICO

Information Commissioner’s Office.

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. ‘Sensitive Personal Data’ is ‘Personal Data’ designated as sensitive personal data under the GDPR.

Work Premises

Such site or sites as may be occupied by Chambers generally (including 6 Pump Court, Temple) or Pascal Bates specifically (including his home address) and used regularly by him as a place to do work or to have work done for him.

GENERAL DATA PROTECTION POLICY

Introduction

Pascal Bates 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 Pascal Bates:

- 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 Pascal Bates' 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:

- Pascal Bates

- All employees or staff of Pascal Bates or Chambers, including volunteers, work experience students or support staff

- All contractors, suppliers and other people working on behalf of Pascal Bates

It applies to all data Pascal Bates 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 Pascal Bates 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

Pascal Bates and everyone who works for Pascal Bates 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

Pascal Bates 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 Data Subjects 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 by statute and will be disposed of appropriately.

Pascal Bates will ensure all Personal Data is non-recoverable from any computer system used by him when that system comes to be disposed of. Chambers will ensure that all Personal Data is non-recoverable from any computer system used by Chambers in work on behalf of Pascal Bates when that system comes to be disposed of.

Data Access and Accuracy

All Data Subjects have the right to access the information Pascal Bates holds about them, except where specific exemptions apply. Pascal Bates will also take reasonable steps ensure that this information is kept up to date.

In addition, Pascal Bates will, himself and through Chambers' staff, ensure that:

- Everyone processing personal information understands that they are required to follow 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

Pascal Bates may share data with agencies such as government departments and other relevant parties.

Other that where the law permits or requires Pascal Bates to disclose data (including sensitive data) without the Data Subject's consent, the Data Subject will be made aware of how and to whom their information will be disclosed. The circumstances where the law permits or requires Pascal Bates to disclose data (including sensitive data) without the Data Subject's consent may be summarised as follows:

- The carrying out a legal duty or as authorised/required by an appropriate government body

- The protection of the vital interests of a Data Subject or other person

- Where the information has already been made public by or with the consent of the Data Subject

- The conduct of any legal proceedings, the defence of any legal rights and the provision of legal advice

- The monitoring for equal opportunities purposes – i.e. race, disability or religion

- The provision of a confidential service where the Data Subject's consent cannot be obtained or where it is reasonable to proceed without consent.

Data Protection Training

Pascal Bates will ensure that, if he has employees, any of his employees who work on data controlled by Pascal Bates are trained in data protection obligations and particularly this Policy annually. Pascal Bates will through Chambers further ensure that any employees of

Chambers who may do work directly or indirectly for him are correspondingly trained in data protection obligations annually.

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

In respect of all employees and all times when they are employed, Pascal Bates keeps and will keep a register of all training provided those employees.

Non-Conformance

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

Any employee, staff member or worker of Pascal Bates 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 who/which processes data controlled by Pascal Bates 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 Pascal Bates via Chambers.

Practical Information on Data Processing

Pascal Bates 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 (if not received directly by Pascal Bates in person) is usually received in Chambers' Work Premises at 6 Pump Court, where it is stored securely in the Clerks' Room or equivalent until collected in person by Pascal Bates. 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 Pascal Bates by first receiving the Personal Data to be forwarded on to Pascal Bates.

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 Pascal Bates' systems, in order that Data Subjects can be

contacted by Pascal Bates, Chambers' clerks and by other members of Chambers (and, if a case needs to be returned to another barrister, by those involved in reasonable efforts made to return it), and for the processing/collection of Pascal Bates' fee invoices.

3. When hard copy papers are passed to Pascal Bates, or created by printing materials received electronically, they will then be stored securely on Work Premises. They may be taken out of Work Premises (for the purpose of Court hearings or otherwise to be worked on remotely) in accordance with Pascal Bates' Mobile Working Policy.

4. When electronic documents or files are passed to Pascal Bates they will be saved onto Pascal Bates' work system, which may use cloud computing to store these documents remotely and/or locally on one or more device (such as a desktop computer, laptop, tablet computer or smartphone).

5. Electronic documents which are processed by Chambers' clerks as well as being passed to Pascal Bates 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 Pascal Bates.

6. When a case is complete, any hard copy papers no longer required will be returned to the professional client if there is one or else consigned to confidential waste. Papers relating to a direct access client's case will generally be retained unless specific alternative arrangements are made for that particular instruction (in which instance secure disposal equivalent to a return to client or confidential waste disposal will be attained).

7. When a case is complete any electronic files storing all data relating to that case will be marked accordingly, and will be reviewed under Pascal Bates' 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 Pascal Bates' legitimate interests as a barrister. Pascal Bates will at all times adhere to the BSB Code of Conduct on client confidentiality.

MOBILE WORKING POLICY

Introduction

This Policy applies to Pascal Bates and any Data Processor instructed on Pascal Bates' practice who may remove case files, papers or other Personal Data from Work Premises for the purposes of work (including, but not limited to, Court hearings).

Hard Copy Materials

Pascal Bates will adhere to the following rules on paper and other hard copy materials:

1. Pascal Bates will not remove client files or Personal Data from Work Premises for any other reason than carrying out legitimate processing activities.

2. All files or case papers leaving Work Premises are to be stored in an appropriately secured manner under the control of the responsible person at all times.

3. Case files or papers will not be left freely available in any common area (be that of a court or other building open to the public, a privately occupied building, or a means of public or private transport) where there is a risk they may be read by other individuals.

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 not 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 away from Work Premises provided that all reasonable precautions are taken to secure the material when not in use. Whilst what precautions are reasonable will depend on the circumstances arising, in the event that there is to be a removal of hard copy papers from Work Premises which is substantial (in terms of the duration of that removal, the quantity of Personal Data removed or the sensitivity of the Personal Data being removed), Pascal Bates may designate in writing further precautions tailored to the instance-specific circumstances.

7. All case files will be moved securely. Where practicable, they will be kept out of sight and stored as inconspicuously as possible. In particular, case files should not be left

in a car unattended except where the risk of removing them to whatever alternative storage is available is less than the risk of leaving them in the car.

8. Pascal Bates will not dispose of hard copy papers that contain any Personal Data (including handwritten notes, post-its etc) away from Work Premises, ensuring instead that any hard copy materials requiring disposal are returned to Work Premises for confidential waste disposal.

9. When no longer needed for the purpose of work away from Work Premises, all hard copy papers will be returned to Work Premises as quickly as reasonably possible.

Electronic Devices

Pascal Bates will adhere to the following rules when processing Personal Data on electronic devices:

1. If accessing emails from a smartphone or tablet, the device will be suitably password-protected and, if appropriate, encrypted.

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/encrypted as appropriate to the device

   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 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 Pascal Bates with the express authorisation of Pascal Bates, and only in particular circumstances necessary for work-related purposes. Where Chambers receives removable storage media carrying data controlled by Pascal Bates from clients or third parties it will hold these securely until collected by Pascal Bates and such removable media will only be transferred in physical form by tracked or registered services such as tracked DX or post.

8. Pascal Bates 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 details the device itself, together with the details and currency of any anti-virus, anti-spyware, encryption or other security software maintained on each machine. Pascal Bates 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, Pascal Bates creates and holds a wide range of recorded information. Records will be properly retained to enable Pascal Bates to meet the business needs of work at the self-employed regulated Bar, to meet the requirements imposed on Pascal Bates by regulators or under 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 Pascal Bates' business

2. The ability of Pascal Bates to defend or instigate legal actions

3. Pascal Bates' ability to comply with statutory obligations

4. Pascal Bates' 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 Pascal Bates 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 Pascal Bates' 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.

Pascal Bates 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 Pascal Bates 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 Pascal Bates 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 Pascal Bates 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 Pascal Bates as a Data Controller and whoever or whatever may act as a Data Processor for Pascal Bates including Chambers, employees on a substantive or temporary contract, service providers, contractors, and any and all associated persons who work for Pascal Bates.

Maximum Retention Period

Unless a record has been marked otherwise, Pascal Bates' policy will be to only retain data for a period of up to 9 years from the conclusion of the case or cases to which it relates. This standard maximum retention period has been formulated on the basis that this allows a client or third party to issue proceedings or a complaint against Pascal Bates within the generally 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. This is a standard maximum period, and nothing about that period shall prevent or inhibit the secure disposal of data or duplicate data earlier than then if the particular circumstances of a case so permit or require (e.g. by the return of some or all of voluminous hard copy case papers to the professional client, following the conclusion of proceedings and the expiry of any appeal period applicable to them, if it is evident that no purpose would be served in retaining them in the circumstances of that case).

The standard maximum retention period has been calculated taking account of:

1. The business need of Pascal Bates' practice

2. Applicable legislation

3. The need for Pascal Bates to respond to complaints

4. Pascal Bates directly or indirectly (e.g. through an insurer) taking or defending legal action

Disposal

What is Disposal?

Pascal Bates is responsible for ensuring that all data held is periodically reviewed at least annually to determine whether any retention periods have expired. Once the retention period has expired, the data will be reviewed and a 'disposal action' determined. In respect of any data retained from prior to the entry into force of this Policy, Pascal Bates will progressively work through that data and assess if for disposal or further retention upon the principles here set out and which would have been applied to it from the outset had that data been received after the entry into force of this Policy.

A 'disposal action' is:

1. The destruction of the record, or

2. The retention of the record for a specific further period in order to facilitate Pascal Bates' 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 Pascal Bates.

The disposal decision will be reached having regard to:

- The on-going business and accountability needs of Pascal Bates' 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 Pascal Bates' practice
- No work is outstanding on any instructions on the case in question or any related case
- No litigation, complaint 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 securely consigned as confidential waste for processing by an approved disposal firm or cross-cut shredded by Pascal Bates. Duplicate hard copies which are no longer required of data which needs to be retained (whether in hard copy or electronic form) may be so consigned at any time. When data no longer falls to be retained at all, steps will be taken to ensure that all hard copies (including security copies, preservation copies and backup copies) are identified and destroyed in that secure manner.

Destruction of Electronic Records

All electronic records will ultimately be either physically destroyed or wiped. Destruction of electronic records by deletion of the files without more will not be sufficient, but data may be deleted pending the eventual physical destruction or wiping of the device in question, in which instance the date of data disposal will be taken as the date of deletion.

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 (Data Subjects) who are the subject of Personal Data held by Pascal Bates are entitled to:

1. Ask what Personal Data Pascal Bates 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 Pascal Bates is meeting his data protection obligations

If a Data Subject contacts Pascal Bates requesting this information, this is called a Subject Access Request. This request is to be responded to promptly and in any event within one month. Pascal Bates can be contacted through Chambers.

Correspondingly, any Data Subject making a Subject Access Request will recognise that the giving of an efficient, brisk, accurate and proportionate response to it depends on the proper and early identification of (i) how Pascal Bates might hold relevant data, (ii) the Data Subject's entitlement to make the Subject Access Request and (iii) the establishment that there are not applicable exemptions requiring or permitting the Subject Access Request to be rejected in whole or in part.

Pascal Bates may check if there are any exemptions contained within the GDPR which require or permit any part of the requested data to be withheld, and may carry out any of the following before releasing data pursuant to a Subject Access Request:

1. Require that any request not made wholly in writing be reduced to written terms.

2. Require satisfactory proof of identification (including photographic identification and/or inspection of original documents) of the Data Subject before sharing any information.

3. Require that the Data Subject identify in writing the case or cases in respect of which s/he believes Pascal Bates may hold his/her Personal Data (e.g. 'High Court proceedings brought by John Smith against Bloggs Builders Limited') and the capacity or capacities in which the individual considers that s/he may have figured in data relating to that case or those cases (e.g. 'as a witness').

4. Require that the Data Subject clarify or further detail in writing any aspect of the Subject Access Request Pascal Bates considers to be unclear.

Pascal Bates will ordinarily provide a copy of all information which falls to be disclosed to the Data Subject pursuant to a Subject Access Request within one calendar month of receipt of all elements of the request (including any which may be additionally required of the Data Subject pursuant to subparagraphs 1 to 4 above).

DATA BREACH MANAGEMENT CHECKLIST

Introduction

This Policy will apply as a Checklist to guide Pascal Bates through the steps necessary upon any data breach or suspected data breach occurring in respect of data for which Pascal Bates 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”*.

Pascal Bates 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 ?

Containment

Record what technical systems have been affected:

1. Emails

2. Cloud or server storage

3. Case or practice management systems

4. Mobile devices

5. Home or Chambers internet access

What can Pascal Bates 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. BSB

9. ICO

10. Professional indemnity insurer

11. CJSM

Sources of Assistance

Does Pascal Bates need to get legal advice ?

Does Pascal Bates need PR assistance in relation to media attention ?

Can Pascal Bates' 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

Pascal Bates

Registered Data Controller Ref No. Z6394031

And

Any Data Controller instructing Pascal Bates to carry out regulated activities as a barrister

Dated

The date to be determined in accordance with clause 6 of this agreement

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 Pascal Bates’ professional client.

Parties

3. This Joint Controllers’ Data Sharing Agreement (“Agreement”) is between:

   (1) Pascal Bates as a Data Controller

   And

   (2) Any Data Controller instructing Pascal Bates

   (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 the earliest of (i) instructions being received by Pascal Bates (or on his behalf) for him to carry out any task appropriate for a barrister and (ii) upon the transfer of any Personal Data to Pascal Bates (or to those acting on his behalf), if such is transferred prior to formal instruction.

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 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

Pascal Bates

Registered Data Controller Ref No. Z6394031

And

Any Data Processor instructed or contracted by Pascal Bates to carry out any form of Data Processing

Dated

The date to be determined in accordance with clause 6 of this agreement

<u>Introduction</u>

1. Pascal Bates will instruct Data Processors to act to process Personal Data for which Pascal Bates is the applicable Data Controller.

2. Because the services require the processing of Personal Data and Sensitive Personal Data, the GDPR is engaged. Pascal Bates 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. Pascal Bates as a Data Controller wishes to engage the services of the Provider as a Data Processor to process Personal Data which Pascal Bates controls as a Data Controller.

Parties

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

(1) Pascal Bates as a Data Controller

And

(2) Any Data Processor (within the meaning of the GDPR) instructed or contracted by Pascal Bates to provide services where Personal Data controlled by Pascal Bates 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 the earliest of (i) Pascal Bates sending instructions to, or contracting with, the Provider to carry out any task involving the processing of Personal Data and (ii) the transfer of any Personal Data to such a Data Processor, if such is transferred prior to formal instruction/contract.

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 Pascal Bates under any Main Contract.

Data Controller Rights and Responsibilities

10. Pascal Bates 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. Pascal Bates remains legally responsible for the Data Processing carried out by the contracted Provider as Data Processor.

13. Pascal Bates 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. Pascal Bates, 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 Pascal Bates 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 Pascal Bates 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 Pascal Bates or process Personal Data in any way or for any purpose that it has not been instructed and authorised by Pascal Bates, or sub-contract a third party to process Pascal Bates' Personal Data without the prior knowledge and written agreement of Pascal Bates, 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 Pascal Bates.

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 Pascal Bates' 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 Pascal Bates' 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 Pascal Bates any information security incidents relating to a personal Data Subject whose Personal Data controlled by Pascal Bates and undertakes to also fully cooperate with Pascal Bates' incident investigation requirements.

24. It is Pascal Bates' 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 Pascal Bates 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 Pascal Bates 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. Pascal Bates 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 Pascal Bates.

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 whose Personal Data I have received 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 Z6394031.

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
- Court, tribunals, arbitrators, adjudicators, mediators and other bodies/individuals who may be vested in a given instance with a decision-making and/or dispute-resolving role.
- My Chambers management and staff who provide administrative services such as clerks
- The BSB 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

Transfers Outside the EEA

I do not generally transfer Personal Date to third countries outside the EEA. If I transfer Personal Data to third countries or international organisations outside the EEA, I do so using identified safeguards, because I need to do so for the purposes of my practice (e.g. in order to operate a cloud computing data storage model, to retrieve emails whilst travelling) and only where I am satisfied that such transferred data is fully protected and safeguarded as required by the GDPR. (For example, I may transfer Personal Data to the USA via Microsoft

Corporation using its Microsoft OneDrive and Office products, having satisfied myself that Microsoft Corporation is accredited under the US-EU Privacy Shield programme.)

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 may 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, making it plain that you are making a Subject Access Request.

Updates

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