Privacy Notice - General Data Protection Regulation ("GDPR")

Please read the following information carefully. This privacy notice contains information about the information collected, stored, and otherwise processed about you and the reasons for the processing. It also tells you who 3VB Services shares this information with, the security mechanisms 3VB Services has put in place to protect your information and how to contact 3VB Services in the event you need further information.

Data Controller

3VB Services Limited ("3VB Services"), the service company of the barristers' chambers of 3 Verulam Buildings ("Chambers") collects, uses and is responsible for personal information about you. 3VB Services are registered with the Information Commissioner's Office (ICO) as a Data Controller for the personal data that we hold and process. Our registered address is Wilmington House, High Street, East Grinstead RH19 3AU, England. Our registration number is 10571837, and our Data Protection Manager (DPM) is our Chambers Director. Our DPM can be contacted at dataprotecton@3vb.com.

Why we process personal data

The information that we hold about you is provided to us by yourself when you seek to use our services, or you are employed by us or work within various capacities. We will tell you why we need the information and how we will use it.

Personal data is any information that can be used to identify an individual, and it can range from the most basic of details such as contact information through to more complex data. Identification can be by the information alone or in conjunction with any other information. The processing of personal data is governed by both the UK General Data Protection Regulation (the UK GDPR) and the Data Protection Act 2018.

Not all personal data is considered equal. There are two different categories: 'personal data' and 'special categories of personal data'.

We collect and process both personal data and special categories of personal data as defined in the UK GDPR. This includes personal data such as;

- Personal and family information, including names, dates of birth, and personal contact details;
- Financial details such as financial status and bank details;
- Records of goods and services relevant to Chambers;
- Records of education, training, and employment;
- Other personal information relevant to the provision of legal services, including information relevant to the specific instructions given in a case.

Sensitive and special data including:

- Information about physical and mental health, including any relevant Covid-19 Track and Trace information;
- Racial or ethnic origin
- Political opinions
- Religious, philosophical, or other beliefs
- Trade union membership
- Sex life or sexual orientation
- Genetic and biometric information of natural persons;

How Do We Collect Information?

In most circumstances you will provide us with personal data when you get in touch with us whether this is to assist your barrister in the provision of legal services or when you are employed by us or are a member of chambers or provide services to us.

3VB Services may also obtain information from third parties, such as members of Chambers, experts, members of the public, your family and friends, witnesses, courts and other tribunals, suppliers of goods and services, investigators, government departments, regulators, public records, and registers. In addition, we may obtain information from other employees, contractors, and referees.

3VB Services complies with its obligations under the UK GDPR:

- by collecting and retaining only data necessary to pursue Chamber's legitimate business interests;
- by ensuring that appropriate technical measures are in place to protect personal data;
- by keeping personal data up to date;
- by storing and destroying data securely.

How 3VB Services Uses Your Personal Information?

3VB Services may use your personal information for the following purposes:

- To direct your enquiries to the appropriate barrister
- To process or support payments for goods and services;
- To maintain the safety, security, and integrity of our services;
- To investigate and address your concerns or any complaints relating to our services;
- Communicating with you about services, news, updates, and events;
- Investigating or addressing legal proceedings relating to your use of our services or as otherwise allowed by applicable law;
- To make statutory returns as required by law;
- To promote and market the services of the Barristers;
- To assess applications for and provide: tenancy, pupillage, mini-pupillage, and work-shadowing opportunities;
- To facilitate work experience;
- To fulfil all regulatory and operational obligations as employers;
- To publish legal judgments and decisions of courts and tribunals;

- To carry out anti-money laundering and terrorist financing checks;
- As otherwise required or permitted by law.

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

Our Legal Basis for Processing Your Personal Information

The UK GDPR requires all organisations that process personal data to have a Lawful Basis for doing so. The Lawful Bases identified in the UK 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 ourselves, or a third party, except where such interests are overridden by the interests, rights, or freedoms of the data subject.

Our Lawful basis is:

- Legal Obligation: 3VB Services is required to process information to comply with various legal obligations including record keeping, administration and regulatory activities. As an employer we also have additional employment related legal obligations.
- Legal Contract: We are required to process personal information to enter into and fulfil various obligations for contracted services or relating to employment contracts.
- Public Interest: The processing is necessary to prevent or detect unlawful acts where it is in the substantial public interest, and it must be carried out without consent so as not to prejudice those purposes.
- Legitimate Interest: We will rely on the legitimate interest of 3VB Services when processing information for the purposes set out above to include the management, administration, and operation of Chambers, for all business development and marketing purposes, to conduct all employment functions and obligations, to comply with all regulatory functions required by professional regulators.
- Consent: On occasion we may rely upon your consent particularly in relation to our marketing activity. At all times you retain the right to withdraw your consent. Where we have relied upon your consent, and you opt to withdraw it this does not invalidate our lawful basis for processing data historically.

Special category processing

If we are processing special categories of data such as medical records, we are entitled by law to do so where it is necessary for the purposes of employment law and to support individuals with a particular disability or medical condition. We may also obtain your consent to process this type of data.

Criminal data processing

On occasion, 3VB Services may process data relating to criminal offences where it is necessary for the purpose of, or in connection with, any legal proceedings; obtaining legal advice; or establishing, exercising, or defending legal rights. We may also request your specific consent to process this type of data.

Who Will 3VB Services Share Your Personal Information With?

It may be necessary to share your information with the following:

- Delivery partners;
- Our business partners, professional advisors, and trade bodies e.g., the Bar Council
- Any other party where we ask you and you consent to the sharing;
- Our legal advisors in the event of a dispute or other legal matter;
- Law enforcement officials, government authorities, or other third parties to meet our legal obligations;
- IT Support services
- Professional advisers and consultants engaged in the course of running of 3VB Services; Regulatory bodies including the Bar Standards Board, Financial Conduct Authority, Information Commissioner's Office (. In the case of the Information Commissioner's Office, there is a risk that your information may lawfully be disclosed by them for the purpose of any other civil or criminal proceedings, without 3VB Services' consent or your consent, which includes privileged information) and the Legal Ombudsman;
- Recruitment agencies;
- Other barristers chambers;
- Prosecution authorities;
- Courts and tribunals;
- Members of 3VB Services including Barristers and trainee Barristers;
- Advisers and other parties involved in any matter you discuss with us, or engage a member of 3VB Services to act on, such as professional clients, lay clients and professional clients;
- Next of kin for employees and members;
- The intended recipient, where you have asked 3VB Services to provide a reference;
- The general public in relation to the publication of legal judgments and decisions of courts and tribunals;

Except for the reasons set out above 3VB Services will not share your personal data with third parties without obtaining your prior consent. Any third parties that we may share your data with are obliged to keep your details securely, and to use them only to fulfil the service they provide on our behalf.

Transfer Of Your Information Outside the European Economic Area (EEA)

All personal data is stored to cloud information storage services in the UK to store your information and/or backup copies of your information so that 3VB Services may access it when it needs to.

It may occasionally be necessary to transfer personal data outside the UK or EEA using appropriate safeguards. This may be, for example, in a situation where you reside outside of the UK or EEA or the role for which you have applied requires a reference from persons, organisations or courts and tribunals outside the UK or EEA. As this privacy notice is of general application it is not possible to provide a definitive list.

If this applies to you and you wish additional precautions to be taken in respect of your information, please indicate this when providing initial instructions.

Some countries and organisations outside the EEA have been assessed by the European Commission and their information protection laws and procedures found to show adequate protection. The list can be found

here. Most do not. If your information must be transferred outside the EEA, then it may not have the same protections and you may not have the same rights as you would within the EEA.

If 3VB Services decides to publish a judgment or other decision of a Court or Tribunal containing your information, then it may be published to the world. 3VB Services will not otherwise transfer personal information outside the EEA except as necessary for the conduct of any legal proceedings.

How Long Do We Keep Your Personal Data?

We retain your personal data while you remain a client, member, pupil, or employee unless you ask us to delete it. Our Data Retention and Disposal Policy details how long we hold data for and how we dispose of it when it no longer needs to be held. We will delete or anonymise your information at your request unless:

- There is an unresolved issue, such as claim or dispute;
- We are legally required to retain the data to meet out legal, statutory, and regulatory obligations;
- There are overriding legitimate business interests, including but not limited to fraud prevention and protecting clients' safety and security.

Your Rights

Under the GDPR, you have a number of rights that you can exercise in certain circumstances. Where those circumstances are established, you may have the right to:

- Ask for access to your personal information and other supplementary information;
- Ask for correction of mistakes in your data or to supplement information 3VB Services holds on you;
- Ask for your personal information to be erased;
- Receive a copy of the personal information you have provided or have this information sent to a third party;
- Object at any time to processing of your personal information for direct marketing;
- Object to the continued processing of your personal information;
- Restrict 3VB Services processing of your personal information.

If you want more information about your rights under the GDPR please see the Guidance from the Information Commissioners Office on Individual's rights under the GDPR.

If you want to exercise any of these rights, or for any further enquiries relating to data protection at 3VB Services please contact dataprotection@3vb.com, phone the Chambers Director at +44 (0) 20 7831 8441 or write to 3 Verulam Buildings, Gray's Inn, London, WC1R 5NT, England, Ref 'Data Protection'.

Marketing and promotion

In relation to personal information collected for marketing purposes, the personal information consists of

- names, contact details, and name of organisation
- the nature of your interest in Chambers' marketing
- your attendance at Chambers events.

This will be processed so that you can be provided with information about Chambers and the Barristers/Mediators/Arbitrators and to invite you to events.

Please note if you wish to unsubscribe from any marketing emails that you have signed up for, you can do so by emailing marketing@3vb.com. It usually takes one working day for this to become effective.

How to make a complaint

You may raise a complaint directly with the Information Commissioners Office on 0303 123 1113 or via email https://ico.org.uk/global/contact-us/email/ or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire. SK9 5AF.

Cookies

Cookies are small text files that are stored on your browser or device by websites, apps, online media, and advertisements. We use cookies to:

- Validate users;
- Remember user preferences and settings;
- Determine frequency of accessing our content;
- Measure the effectiveness of advertising campaigns; and
- Analyse site visits and trends.

Future Processing

3VB Services does not intend to process your personal information except for the reasons stated within this privacy notice. In the event of changes, this privacy notice will be updated.

We will occasionally update our Privacy Notice. When we make significant changes, we will publish the updated Notice on our website (www.3vb.com). This Privacy Notice was published on 25 May 2018 and last updated on 1 December 2023.

Contact Details

If you have any questions about this privacy notice or the information 3VB Services holds about you, please contact 3VB Services using the contact details below.

The best way to contact 3VB Services is:

- to email dataprotection@3vb.com ;
- to phone the Chambers Director at +44 (0) 20 7831 8441;
- to write to 3 Verulam Buildings, Gray's Inn, London, WC1R 5NT, England, Ref Data Protection.

DATA PROTECTION POLICY

Introduction

3 Verulam Buildings and its service company, 3VB Services Limited ("Chambers") are required to comply with the law governing the management and storage of personal data, which is outlined in the UK GDPR and the Data Protection Act 2018 (DPA). For this reason, protection of personal data and respect for individual privacy is fundamental to the day-to-day operations of Chambers. Compliance with the Uk GDPR is overseen by the UK data protection regulator which is the Information Commissioner's Office (ICO). Chambers is accountable to the ICO for its data protection compliance.

Policy Statement

The Head(s) of Chambers, members of Chambers, pupils and employees are committed to compliance with all relevant EU and UK laws in respect of personal data, and the protection of the rights and freedoms of individuals whose information we collect and process in accordance with the UK GDPR.

Scope

The UK GDPR and this policy apply to all our personal data processing functions, including those performed on partners,' customers,' clients,' employees' and suppliers' personal data, and any other personal data we process from any source.

This policy applies to all employees (permanent and temporary), agency, and contract staff. Any breach of the UK GDPR will be dealt with under our disciplinary policy and may also be a criminal offence, in which case the matter will be reported as soon as possible to the appropriate authorities.

It is also applicable to Members when they are processing Chambers data/ on and behalf of Chambers by virtue of their membership of Chambers, where sitting on a Chambers Committee or for other internal matters associated with their membership.

Partner organisations and third parties working with or for us which have or may have access to personal data will be expected to adhere to all obligations imposed by data protection legislation. No third party may access personal data held by us without having first entered into a Data Sharing Agreement which imposes on the third-party obligations no less onerous than those to which we are committed, and which gives us the right to audit compliance with the Agreement.

Responsibility

Everyone in Chambers (and any third party to whom this policy applies to) is responsible for ensuring that they comply with this policy. Failure to do so may result in disciplinary action.

Data Protection Manager (DPM)

Chambers has appointed the Chambers Director as its Data Protection Manager (DPM). This is not a statutory role. The Chambers Director's responsibilities within this role include:

- Developing and implementing data protection policies and procedures;

- Arranging regular data protection training for all staff and members which is appropriate to them;
- Acting as a point of contact for all members, associate members, pupils, and staff on data protection matters;
- Monitoring Chambers' compliance with its data protection policy and procedures;
- Promoting a culture of data protection awareness;
- Assisting with investigations into data protection breaches and helping Chambers to learn from them;
- Advising on Data Protection Impact Assessments; and
- Liaising with the relevant supervisory authorities as necessary (i.e., the Information Commissioner's Office in the UK).

Definitions

Data Protection Principles

All processing of personal data must be conducted in accordance with the Data Protection Principles as set out in the UK GDPR and outlined below. Our policies and procedures are designed to ensure compliance with these Principles.

Principle 1

Personal data must be processed lawfully, fairly, and transparently.

Lawful – we need to identify a lawful basis before we can process personal data, for example, consent.

Fairly – in order for processing to be fair, we have to make certain information available to Data Subjects. This applies whether the personal data was obtained directly from Data Subjects or from other sources.

Transparently – the UK GDPR includes rules on giving privacy information to Data Subjects. These are detailed and specific, placing an emphasis on making privacy notices understandable and accessible. Information must be communicated to the Data Subject in an intelligible form using clear and plain language.

Principle 2

Personal data can only be collected for specific, explicit, and legitimate purposes

The data we obtain for specified purposes must not be used for a purpose that is incompatible with those formally notified to the ICO as part of our UK GDPR register of processing.

Principle 3

Personal data must be adequate, relevant, and limited to what is necessary for processing

We cannot collect information that is not strictly necessary for the purpose for which it is obtained.

Principle 4

Personal data must be accurate and, where necessary, kept up to date.Every reasonable step must be taken to ensure that personal data that are inaccurate are erased or rectified without delay. Data that is stored by us must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that it is accurate.

Principle 5

Personal data must be kept in a form such that the Data Subject can be identified only as long as is necessary for processing. We should only hold personal data for as long as we need it.

Principle 6

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

Demonstrating Accountability

The GDPR includes provisions that promote Accountability and Governance. These complement the GDPR's transparency requirements. Accountability requires us to demonstrate that we comply with the GDPR Principles.

We will demonstrate compliance with the GDPR Principles by implementing and adhering to data protection policies, implementing technical and organisational measures, as well as adopting techniques such as Data Protection by Design, Data Protection Impact Assessments, breach notification procedures and incident response plans.

Data Subjects' Rights

The UK GDPR provides the following rights for individuals in relation to their personal data:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

Data Subjects may make Subject Access Requests relating to their personal data. Our Subject Access Request Policy describes how we will ensure that our response to the request complies with the requirements of the GDPR.

Our DPM is responsible for responding to requests for information from Data Subjects within one calendar month in accordance with our Subject Access Request Policy. This can be extended to two months for

complex requests in certain circumstances. If we decide not to comply with the request, the DPM must respond to the Data Subject to explain our reasoning and inform them of their right to complain to the ICO and seek judicial remedy.

Data Subjects have the right to complain to us about the processing of their personal data, the handling of a Subject Access Request and to appeal against how their complaints have been handled.

Consent

We understand 'consent' to mean that it has been explicitly and freely given, and it is a specific, informed, and unambiguous indication of the Data Subject's wish that, by statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The Data Subject can withdraw their consent at any time.

We also understand 'consent' to mean that the Data Subject has been fully informed of the intended processing and has signified their agreement while in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing.

Consent cannot be inferred from non-response to a communication. As Data Controller, we must be able to demonstrate that consent, where necessary, was obtained for the processing operation.

For Sensitive Personal Data, explicit written consent of Data Subjects must be obtained unless an alternative legitimate basis for processing exists.

Where we provide online services to children under the age of 13, parental or custodial authorisation must be obtained.

Collection of Data

All data collection forms (electronic and paper-based), including data collection requirements in new information systems, must include a fair processing statement or a link to our Privacy Notice and be approved by the DPM.

Accuracy of Data

Our DPM is responsible for ensuring that all employees are trained in the importance of collecting accurate data and maintaining it.

Employees are required to notify the Head of Finance and Operations of any changes in their personal circumstances which may require personal records be updated accordingly.

Our DPM is responsible for ensuring that appropriate procedures and policies are in place to keep personal data accurate and up to date, considering the volume of data collected, the speed with which it might change and any other relevant factors.

Our DPM is responsible for making appropriate arrangements where third-party organisations may have been passed inaccurate or out-of-date personal data to inform them that the information is inaccurate

and/or out of date and is not to be used to inform decisions about the individuals concerned; and for passing any correction to the personal data to the third party where this is required.

Security of Data

All personal data is accessible only to those who need to use it. All personal data is treated with the highest security as set out in our Data Security Policy.

No less than annually our DPM will carry out a risk assessment, considering all the circumstances of our data controlling and processing operations. In determining appropriateness of all technical and organisational security measures, the DPM will consider the extent of possible damage or loss that might be caused to individuals (e.g., staff, clients, or members) if a security breach occurs, the effect of any security breach on our organisation itself, and any likely reputational damage, including the possible loss of customer trust.

It is strictly prohibited to remove personal data from our premises for any reason other than carrying out legitimate processing activities.

Processing of personal data 'off-site' presents a potentially greater risk of loss, theft, or damage to personal data and the precautions that must be taken are set out in our Working from Home Policy.

All employees are responsible for ensuring that any personal data that we hold and for which they are responsible is kept securely and is not, under any condition, disclosed to any third party unless that third party has been specifically authorised by us to receive that information and has entered into a Data Sharing Agreement.

Disclosure of Data

All requests to provide personal data must be supported by appropriate paperwork and all such disclosures must be specifically authorised by the DPM.

We must ensure that personal data is not disclosed to unauthorised third parties, which includes family members, friends, government bodies, and, in certain circumstances, the Police. All employees should exercise caution when asked to disclose personal data held on another individual to a third party.

Retention and Disposal of Data

We shall not keep personal data in a form that permits identification of Data Subjects for a longer period than is necessary in relation to the purpose(s) for which the data was originally collected.

The retention period for each category of personal data is set out in our Data Retention and Disposal Policy.

Personal data will be retained in line with our Data Retention and Disposal Policy and, once its retention date is passed, it must be securely destroyed as set out in this policy.

On at least an annual basis, our DPM will review the retention dates of all the personal data processed by our organisation and will identify any data that is no longer required. This data will be securely archived, deleted, or destroyed in line with our Retention and Disposal Policy.

Where personal data is archived, it will be encrypted and/or pseudonymised in order to protect the identity of the Data Subject in the event of a data breach.

Our DPM must specifically approve any data retention that exceeds the retention periods defined in our Data Retention and Disposal Policy and must ensure that the justification is clearly identified and recorded.

We may store data for longer periods if the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the implementation of appropriate technical and organisational measures to safeguard the rights and freedoms of the Data Subject. Any such retention must be approved in advance by the DPM.

International Data Transfers

Under UK GDPR, transfers of personal data outside of the European Economic Area can only be made if specific safeguards exist.

Our data is stored only in the UK. However, it may occasionally be necessary to transfer personal data outside the UK or EEA using appropriate safeguards. This may be, for example, in a situation where the client resides outside of the UK or EEA or the role for which we have applied requires a reference from persons, organisations or courts and tribunals outside the UK or EEA. We have satisfied ourselves that the conditions laid down in the Regulations are complied with by the controller and processor by:

1. An adequacy decision, or
2. Binding corporate rules, or
3. Model contract clauses, or
4. Exceptions
    - the Data Subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the Data Subject due to the absence of an adequacy decision and appropriate safeguards:
    - the transfer is necessary for the performance of a contract between the Data Subject and the controller, or the implementation of pre-contractual measures taken at the Data Subject's request;
    - the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Data Subject between the controller and another natural or legal person:
    - the transfer is necessary for important reasons of public interest:
    - the transfer is necessary for the establishment, exercise, or defence of legal claims; and/or
    - the transfer is necessary to protect the vital interests of the Data Subject or of other persons, where the Data Subject is physically or legally incapable of giving consent.

Data Processed Register

Our Register of Data Processed and Retention Dates records:

- each type of personal data:
- why it is collected:
- the lawful grounds for processing:
- where it is held:
- the Responsible Person for the data:
- its Review Date; and
- how it is kept accurate.

Data Protection Impact Assessments (DPIA)

Where a type of processing, using new technologies and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of living peoples, we shall, prior to the processing, carry out a Data Protection Impact Assessment of the envisaged processing operations. All DPIAs should be led by or overseen by the DPM.

Where, as a result of a DPIA it is clear that we are about to commence processing of personal data that could cause damage and/or distress to the Data Subjects, the decision as to whether or not we may proceed must be referred to senior management for approval to proceed.

Our DPM shall, if there are significant concerns, either as to the potential damage or distress, or the quantity of data concerned, refer to the ICO for guidance and advice.

Breaches

A personal data 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".*

Everybody working in, for and with Chambers has a duty to report any actual or suspected data protection breach without delay to their manager and the Chambers Director, or one of the Senior Practice Managers in his absence. Chambers' breach reporting procedure can be found in Chambers Incident Management Plan.

Breaches will be reported to the Information Commissioner's Office (ICO) by the Chambers Director or by one of the Senior Practice Managers in his absence without undue delay and not later than 72 hours after having become aware of the breach, unless Chambers is able to demonstrate that the personal data breach is unlikely to result in a risk to the rights and freedoms of data subjects.

The Chambers Director will maintain a central register of the details of any data protection breaches.

Complaints

Complaints relating to breaches of the UK GDPR and/ or complaints that an individual's personal data is not being processed in line with the data protection principles should be referred to the Chambers Director without delay.

Penalties

It is important that everybody working for Chambers understands the implications for Chambers if we fail to meet our data protection obligations. Failure to comply could result in:

- Criminal and civil action;
- Fines and damages;
- Personal accountability and liability;
- Suspension/withdrawal of the right to process personal data by the ICO;
- Loss of confidence in the integrity of the Chambers' systems and procedures;

- Irreparable damage to Chambers' reputation.

Note: Chambers could be fined up to €20,000,000, or up to 4% of the total annual turnover of the preceding financial year, whichever is higher.