Rebecca Dix customer privacy notice

This privacy notice tells you what to expect me to do with your personal information.

Contact details

Post

Chambers Of Moore & Christopher, 5 Paper Buildings, Temple, LONDON, EC4Y 7HB, GB

Email

rd@5pb.co.uk

What information I collect, use, and why

We collect or use the following personal information for the **operation of client or customer accounts**:

- Names and contact details
- Purchase or service history

We collect or use the following personal information **for the prevention, detection, investigation or prosecution of crimes**:

- Names and contact information

- Client accounts and records
- Video recordings of public areas
- Audio recordings of public areas
- Video recordings of private or staff only areas
- Audio recordings of private or staff only areas
- Call recordings
- Dashcam footage - outside vehicle
- Dashcam footage - inside vehicle
- Financial information eg for fraud prevention or detection
- Location data
- Previous criminal convictions or investigations

We also collect or use the following information **for the prevention, detection, investigation or prosecution of crimes**:

- Racial or ethnic origin
- Political opinions
- Religious and philosophical beliefs
- Trade Union membership
- Genetic information
- Biometric information (where used to identify someone)
- Health information
- Sex life and sexual orientation

We collect or use the following personal information for **information updates or marketing purposes**:

- Names and contact details

- Addresses
- Profile information

We collect or use the following personal information for **recruitment purposes**:

- Contact details (eg name, address, telephone number or personal email address)
- Employment history (eg job application, employment references or secondary employment)
- Education history (eg qualifications)
- Details of any criminal convictions (eg Disclosure Barring Service (DBS), Access NI or Disclosure Scotland checks)

We collect or use the following personal information for **dealing with queries, complaints or claims**:

- Names and contact details
- Witness statements and contact details
- Relevant information from previous investigations
- Correspondence

Lawful bases and data protection rights

Under UK data protection law, we must have a "lawful basis" for collecting and using your personal information. There is a list of possible lawful bases in the UK GDPR. You can find out more about lawful bases on the ICO's website.

Which lawful basis we rely on may affect your data protection rights which are in brief set out below. You can find out more about your data protection rights and the exemptions which may apply on the ICO's website:

- **Your right of access** - You have the right to ask us for copies of your personal information. You can request other information such

as details about where we get personal information from and who we share personal information with. There are some exemptions which means you may not receive all the information you ask for. You can read more about this right here.

- **Your right to rectification** - You have the right to ask us to correct or delete personal information you think is inaccurate or incomplete. You can read more about this right here.
- **Your right to erasure** - You have the right to ask us to delete your personal information. You can read more about this right here.
- **Your right to restriction of processing** - You have the right to ask us to limit how we can use your personal information. You can read more about this right here.
- **Your right to object to processing** - You have the right to object to the processing of your personal data. You can read more about this right here.
- **Your right to data portability** - You have the right to ask that we transfer the personal information you gave us to another organisation, or to you. You can read more about this right here.
- **Your right to withdraw consent** – When we use consent as our lawful basis you have the right to withdraw your consent at any time. You can read more about this right here.

If you make a request, we must respond to you without undue delay and in any event within one month.

To make a data protection rights request, please contact us using the contact details at the top of this privacy notice.

Our lawful bases for the collection and use of your data

Our lawful bases for collecting or using personal information for the **operation of client or customer accounts** are:

- Consent - we have permission from you after we gave you all the relevant information. All of your data protection rights may apply, except the right to object. To be clear, you do have the right to withdraw your consent at any time.

- Contract – we have to collect or use the information so we can enter into or carry out a contract with you. All of your data protection rights may apply except the right to object.

Our lawful bases for collecting or using personal information **for the prevention, detection, investigation or prosecution of crimes** are:

- Consent - we have permission from you after we gave you all the relevant information. All of your data protection rights may apply, except the right to object. To be clear, you do have the right to withdraw your consent at any time.
- Contract – we have to collect or use the information so we can enter into or carry out a contract with you. All of your data protection rights may apply except the right to object.
- Legal obligation – we have to collect or use your information so we can comply with the law. All of your data protection rights may apply, except the right to erasure, the right to object and the right to data portability.
- Legitimate interests – we're collecting or using your information because it benefits you, our organisation or someone else, without causing an undue risk of harm to anyone. All of your data protection rights may apply, except the right to portability. Our legitimate interests are:
    - Provision of legal services and advice, whether that be defending the data subject during an investigation and or court proceedings or investigating and prosecuting the data subject on behalf of the Crown. The collection and use of personal information are limited to use in the criminal proceedings and any subsequent appeals or enquiry.
- Public task – we have to collect or use your information to carry out a task laid down in law, which the law intends to be performed by an organisation such as ours. All of your data protection rights may apply, except the right to erasure and the right to portability.

Our lawful bases for collecting or using personal information for **information updates or marketing purposes** are:

- Consent - we have permission from you after we gave you all the relevant information. All of your data protection rights may apply, except the right to object. To be clear, you do have the right to withdraw your consent at any time.

Our lawful bases for collecting or using personal information for **recruitment purposes** are:

- Consent - we have permission from you after we gave you all the relevant information. All of your data protection rights may apply, except the right to object. To be clear, you do have the right to withdraw your consent at any time.
- Contract – we have to collect or use the information so we can enter into or carry out a contract with you. All of your data protection rights may apply except the right to object.
- Legitimate interests – we're collecting or using your information because it benefits you, our organisation or someone else, without causing an undue risk of harm to anyone. All of your data protection rights may apply, except the right to portability. Our legitimate interests are:
    - The information is acquired to support their written application when applying to join Chambers or to seek work experience.

Our lawful bases for collecting or using personal information for **dealing with queries, complaints or claims** are:

- Contract – we have to collect or use the information so we can enter into or carry out a contract with you. All of your data protection rights may apply except the right to object.
- Legal obligation – we have to collect or use your information so we can comply with the law. All of your data protection rights may apply, except the right to erasure, the right to object and the right to data portability.

Where we get personal information from

- Legal bodies or professionals (such as courts or solicitors)

How long we keep information

I retain your personal data while you remain a client and seven years thereafter your matter has concluded. A record is kept to identify when your records will be deleted. I will delete your information at your request unless:

- There is an unresolved matter, such as a claim, appeal or dispute;
- I am legally required to retain the data; and/or
- There are overriding legitimate business interests to do so.

I dispose of any hard copy documents which contain information by placing them into confidential waste bags at 5 Paper Buildings, which are sent for secure disposal.

Security of storage of information

This part of my Privacy Notice relates to the retention and storage of all personal data held in hard copy, i.e. on paper, on physical devices like USBs, CDs, DVDs, tablets and smartphones and the retention and use of electronic data.

It applies to all use of information and information technology at 5 Paper Buildings and at my primary residence.

I implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk and severity of its processing to the data subject.

I store all the information in digital format securely via the Cloud (as above) which I access only via encrypted and password protected devices.

I also have regard to the following minimum levels of security:

a) All personal computers/devices used for work must be protected by up-to-date anti-virus and anti-spyware software, subjected to regular virus scans, and protected by a firewall appropriate for the computer used.
b) The operating software must be checked regularly to ensure that the latest security updates are downloaded.
c) Access to all computers must be password protected.
d) Particular care must be taken to avoid potential infection by malware, e.g. by downloading software other than from trusted sources.

e) Work-in-progress should be regularly backed up, and backup media should be locked away securely.
f) Computers used for working on personal data at home should be protected from unauthorised and unrestricted access by third parties, including family members.
g) The use of removable storage media (such as memory sticks, CD-ROMs, removable hard disk drives and PDAs) are only to be used in particular circumstances and only encrypted removable storage media devices are permitted.
h) Laptop computers must be encrypted to such standards as may be approved by my IT provider.

I also have regard to the following:

Email and internet use

1. Always check the address line before sending a message and check it is being sent to the correct person. Ensure the automatic email address filler is turned off or used with extreme caution.
2. Always encrypt any attachments which contain special category data, as defined under the GDPR.
3. Consider using an email 'delay' function when sending any emails which contain special category data, as defined under the GDPR.
4. Delete electronic mail messages when they are no longer required.
5. Personal private emails must be saved in a separate folder from work-related emails. Clearly mark all emails that are of a personal nature as 'personal'.
6. Do not open email attachments received from unknown senders as these may contain viruses, email bombs, Trojan horse code or some other form of malware.
7. Do not forward electronic mail messages that have been sent to you containing personal data, including any personal data sent to you in respect of any chambers committee you may sit on (as defined by the GDPR) to other individuals or groups without the permission of the originator.
8. Do not unnecessarily send excessively large electronic mail messages or attachments.

Passwords

1. All devices must be protected with a password.
2. Passwords must be kept secure.
3. Passwords must be [at least 7 characters long and include alpha, numeric and at least one other character].
4. Passwords should never be displayed on screens.

All information stored in hard copy format at 5 Paper Buildings is secured by the following means:

- in my dedicated room, access to which is from a communal staircase through a 'double door', the first of which is secured by a key and the second by a key code. Entrance to the building (and hence the communal staircase) is via a 24-hour electronically secure door.

Occasionally I store information at my primary residence, in a locked cupboard for which only I have a key.

Where I take hard copy files containing personal data out of my secure office or primary residence, I take appropriate security precautions to guard against theft, loss or inappropriate access – which includes ensuring, so far as is reasonably practicable, that no-one could read the files which I am working on, where ever that might be.

If I undertake the external transfer of personal data, I consider whether such a transfer is authorised under any relevant Data Sharing Agreement or is otherwise required by or permitted under the General Data Protection Regulation. This includes considering the purpose, fairness and transparency of any transfer must always be considered.

Where external data sharing has been considered necessary or is permitted, I take appropriate security precautions to minimise the risks of loss of data and/or accidental third-party disclosure.

I keep the circumstances of the security of my storage of information under review. I assess the potential risks for unauthorised access to personal data and to define appropriate actions to eliminate, or at least mitigate, the risk of unauthorised access.

If, despite all of the above, the security of personal data or IT systems is compromised, or where I am aware that there have been any suspected security weaknesses or threats, I will immediately review the circumstances and, where appropriate, take remedial action.

As the Date Controller, I will decide whether the particular circumstances are serious enough to inform the Information Commissioner's Office.

Who we share information with

Data processors

5 Paper Buildings Legal services, London

This data processor does the following activities for me: Processes invoices and payments, manages our IT systems, stores HR records, shares data from legal services providers and the Crown and manages case allocation.

Others we share personal information with

- Other financial or fraud investigation authorities
- Professional or legal advisors, including pupils and mini-pupils.
- Regulatory and law enforcement authorities
- Third parties:
    - Instructed experts during the course of a criminal investigation, prosecution and appeal.
    - Legal directories for the purpose of professional development

How to complain

If you have any concerns about our use of your personal data, you can make a complaint to us using the contact details at the top of this privacy notice.

If you remain unhappy with how we've used your data after raising a complaint with us, you can also complain to the ICO.

The ICO's address:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Helpline number: 0303 123 1113

Website: https://www.ico.org.uk/make-a-complaint

Last updated

20 December 2024