DATA PROTECTION POLICY OF SAMIR AMIN

6 November 2022

1. I am a Data Controller under the General Data Protection Regulation, and am registered with the Information Commissioner's Office as a Data Controller.

2. This policy applies to all the personal data that I hold relating to identifiable individuals.

3. In case of any queries or questions in relation to this policy please contact me, Samir Amin.

4. I recognise that I control and am personally responsible for compliance with the GDPR in relation to the personal data that I control, which is all the personal data coming to me in the course of my practice. I recognise this as a non-delegable responsibility. I do not process data for clients.

5. The categories of data subjects whose data I collect are my own clients and all persons involved in the cases with which I deal. This may include sensitive data of the type listed in Art 9 of the GDPR. It includes all data which naturally comes to me in the course of my practice as a barrister. For example—

    a. I will inevitably process the personal data of my client including their name, address and other personal data which I am given in relation to them by either them or my Instructing Solicitors;

    b. I may process the personal data of my opponents, which might come to me in the form of witness statements, correspondence, mediation, evidence or

other forms and which usually form part of the factual matrix of the advice which I am giving or a case in which I am acting; and

c. I may process the personal data of third parties, which might come to me in the form of witness statements, correspondence, mediation, evidence or other forms and which usually form part of the factual matrix of the advice which I am giving or a case in which I am acting.

6. Employees of and contractors employed by No5 Chambers Limited will have access to some of the data which I control. Although I recognise the non-delegable nature of my responsibility, I consider that No5 Chambers Limited's own policies are adequate and appropriate. I therefore not intend to lay down any further or different policies in respect of such employees and contractors.

7. Data controlled by me will sometimes be shared with other data controllers, such as solicitors and other barristers. Where such other professionals are under a regulatory obligation of their own to comply with the GDPR, I will assume that they will comply with it unless there is any reason to suggest otherwise.

8. In the case of data processors who are not employees of No5 Chambers or are not professionals subject to their own regulation as aforesaid, I will ensure that everyone processing personal data which I control understands that they are responsible for following best data protection practice, are appropriately trained to do so and are appropriately supervised. Where appropriate, I will enter into data processing agreements to promote best data protection practice by those to whom I entrust data.

General Data Protection Policy

9. Terms used in this policy which are defined terms in the GDPR have that defined meaning.

10. I will process personal data in line with the principles set out within Art 5.

11. I shall ensure that data is processed lawfully within the meaning of Art 6. In particular, the data will be processed lawfully because one or more of the following will usually apply (but may occasionally be processed for lawful reasons other than those set out below)—

    a. There will be specific and informed consent – for instance, when my client gives me their personal data in the course of instructing me or where a witness gives me personal data for the purposes of taking a proof of evidence;

    b. Processing the personal data of my client is necessary for me to perform the contract between me and my client – namely, the retainer between me and my client for my services as a barrister;

    c. The processing is necessary for compliance with a legal obligation – for instance, disclosure pursuant to a court order; or

    d. Processing is necessary for the purposes of the legitimate interests pursued by myself or by a third party.

12. Where the personal data which I control is special category data I will, in addition to having a lawful reason for processing it, ensure that one or more of the conditions in Art 9(2) is met. In relation to the work which I do, the relevant conditions are likely to be Art 9(2)(a), (b), (e) and (f).

13. The reality of my work as a self-employed member of the Bar is that—

a. I acquire large amounts of personal data. That personal data might be recorded in the form of instructions, attendance notes, personal notes which I use for preparation, application notices, statements of case, mediation statements, witness statements, proofs of evidence, skeleton arguments, opinions, transcripts, emails, texts, other correspondence and many other means both physically and electronically. In relation to some of these documents, I will also be provided with similar ones prepared by my opponent;

b. Some of that personal data might be relevant to a case. Some of it might not. Some of it might be thought relevant, but ultimately might not turn out to be so. Some of it may not at first seem relevant, but later might become so;

c. Some of the personal data will be made public – for instance if put before a court sitting in public. Some of it might remain confidential and/or known only to a small class of persons (such as the parties to litigation and their legal representatives);

d. I consider it is necessary to keep, and that I have a legitimate interest in keeping, the documents and information which I am given or create during the course of, or related to, an instruction or potential instruction. With regards to this—

    i. This is most obviously necessary for ensuring that I am able to defend myself in the event of a complaint being made. The maximum limitation period for a claim which I am likely to face as a result of my work as a barrister is 15 years from the date of the act complained of. Any one document, annotation or attendance note may turn out to be key evidence in such a situation; and

ii. I will always respect the confidentiality and often privileged nature of information imparted to me in the course of an instruction. However, I am entitled to retain and use general knowledge (for instance, the law, best practice or procedure) which I acquire throughout the course of an instruction for my own purposes (for instance, in order to advise another client on a similar matter). Such knowledge may be recorded in any one, or more, of the documents referred to in paragraph 13(a) above;

iii. In relation to clients which instruct me on a 'direct access' basis, I have a regulatory obligation to either myself, or take reasonable steps to ensure that my client will, retain for at least seven years after the date of the last item of work done: copies of all instructions (including supplemental instructions); copies of all advices given and documents drafted or approved; the originals, copies or a list of all documents enclosed with any instructions; and notes of all conferences and of all advice given on the telephone; and

iv. To be clear, I consider that keeping documents is necessary for the legitimate purposes of retaining knowledge, experience and expertise; developing professionally; complying with legal and professional requirements; and ensuring that any records of historic value are preserved *inter alia*.

e. In relation to redacting and/or erasing specific personal data contained within documents—

i. I consider that doing so may compromise the integrity of documents to such an extent that I may not be able to meet my regulatory requirements or defend myself in the event of a complaint; and

ii. It is generally not practicable and not proportionate for me to filter out and/or erase personal data when it is contained in documents (both physical and electronic) which I consider that I have a legitimate interest in keeping before, during and/or after an instruction. Such a task would be nearly impossible in the vast majority of matters which I work on. For instance, after the end of a case, those documents referred to in paragraph 13(a) above may run to hundreds if not thousands of pages and, in addition to this, there may be thousands of pages of evidence which are necessary to give context to them.

f. However, I bear in mind that the way I deal with personal data must be proportionate to my legitimate interests (if that is the lawful reason which I rely on for retaining personal data). Therefore, in appropriate cases where I consider that the interests of the data subject outweigh my own, I may adopt a different approach to the retention of documents and personal data. Such an approach might involve irretrievably disposing of the documents, or redacting certain personal data. Each case will depend on its own facts and, if I deem it necessary and possible, the course of action will be determined in consultation with the data subject.

14. Therefore—

a. When instructions have been received and work upon them is not yet complete, I may collect, retain, access, use and communicate the personal data for the purposes of delivering my services;

b. When instructions have been fulfilled, I will retain the personal data only for one or more of the Art 6 reasons. Whilst hard-copy documents will usually be disposed of mere months after the end of an instruction, electronic documents (including electronic copies of hard-copy documents)

are likely to be retained by me indefinitely and in any event for at least fifteen years;

c. If the reason why I retain personal data is because I consider that I have a legitimate interest in preserving that document, my interest in the personal data contained within it is highly likely to be only incidental to my interest in the remainder of the document; and

d. I will not further process data in a manner incompatible with the above but may use it for purposes including the following:

    i. to provide legal services to my clients, including the provision of legal advice and representation;

    ii. to keep accounting records and carry out office administration;

    iii. to take or defend legal or regulatory proceedings or to exercise a lien;

    iv. to respond to potential complaints or make complaints;

    v. to check for potential conflicts of interest in relation to future potential cases;

    vi. to promote and market my services;

    vii. to carry out anti-money laundering and terrorist financing checks;

    viii. to train other barristers and when providing work-shadowing opportunities;

    ix. to respond to requests for references;

    x. when procuring goods and services; and

    xi. as required or permitted by law.

15. I will ensure that so far as it is necessary and within my reasonable power to do so, the personal data is kept up to date.

16. I will keep personal data for only so long as the lawful reason for doing so persists.

17. I will take appropriate technical and organisational security measures to safeguard personal data

18. I will not transfer information outside the UK except by communicating it to a client or his/her/its authorised representative abroad.

19. I will set out clear procedures for responding to requests for information.

20. I will ensure that the rights of people about whom information is held, can be fully exercised under the GDPR.

Data Storage and access

The data

21. The data I control may be divided into the following groups, according to how and where it is kept. This categorisation is not intended to be exhaustive—

    - Hard copy documents;

    - Electronic files stored in a Dropbox account to which only I have access and which only syncs with a laptop to which only I have access;

    - Documents open for the purpose of working on them, and therefore visible on a screen or desk;

- Electronic correspondence, such as emails and sometimes texts. I receive electronic correspondence on my phone, tablet and laptop; and

- Contact details of clients including personal data such as name/address and financial information relating to billing. This data is kept for me by No5 Chambers.

The devices

22. The devices which I use to access electronic personal data are:

- A laptop running Windows 10 which is usually with me during working hours, but otherwise at home;

- An iPhone which is nearly always with me; and

- An iPad which is usually left at home.

23. I occasionally receive data from solicitors or lay clients on external media such as USB sticks. Very occasionally, I may wish to copy data to external media.

Third parties

24. Occasionally employees of Cloud Systems Group access my devices for maintenance and similar purposes, but only in my presence and under my supervision.

Security

Objectives

25. My security objectives are to ensure:

- Confidentiality of information – access to information is restricted to those persons with appropriate authority to access it.

- Integrity of information – information shall be complete and accurate.

- Availability of information – information shall be available and delivered to the right person at the time when it is needed.

Hard copy documents

26. I usually need papers with me wherever I am working, which might be in chambers, at home, in court, at others' offices, while travelling or in hotels.

27. All papers will be moved securely between these locations. On public transport they will not be left unattended unless I absolutely have no choice, in which case they will be secured in a locked suitcase and kept as close to me as possible. Papers left in an unattended car will be stored out of sight. This will only occur where necessary and for brief periods of low risk. Case files will not be left in a car overnight.

28. Papers will never be left freely available in any common area in circumstances where there is a real risk that they may be read by unauthorised individuals. They will never be opened in circumstances where there is such a risk.

29. I take papers home where I often work. I am satisfied that my home is most unlikely to be targeted for the purposes of stealing personal data and that my case papers are unlikely to be of interest to a casual burglar.

30. A special note on papers left in chambers:

a. The GDPR is in its infancy and there is therefore a certain amount of uncertainty over its scope and meaning. It has been suggested by some that: a). Under no circumstances should electronic papers be kept unredacted; and b). Under no circumstances should hard-copy papers be left in chambers unless they are in a locked cupboard – and one person has even suggested to me that that cupboard should be fireproof;

b. I have addressed above my policy, and the reasons for it, in relation to the redacting/erasing of personal data contained in electronic documents. I now address here my policy on the security of papers within the confines of chambers. My risk assessment is that the possibility of breach is very low;

c. Principle (f) of the GDPR requires that I process data *"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"*;

d. It has been the case for at least decades that barristers feel comfortable in leaving hard copy papers in certain areas of chambers (such as on a shelf in an office) with confidence that those papers will not be read by unauthorised individuals. As far as I am aware, this approach has not previously been questioned as constituting inappropriate security;

e. I share an office in chambers with a small group of other barristers. When they are in chambers, my papers are only likely to be stored on my desk, on a shelf in my office or in my personal cupboard or pigeon hole. I am completely satisfied, given that all other barristers and staff of No5 are aware of the importance of confidentiality, privilege and data protection, and given the security measures taken by No5 Chambers in London, that

personal data which I control is not at risk of breach whilst stored or opened here; and

f. I therefore do not consider it is necessary to go anywhere near as far as attempting to install shutters on the shelves in my office or a locked cupboard (fireproof or not). I will look into installing a lock on the actual door to the office which I share, but this might not be possible in all of the circumstances and might be beyond my control.

Dropbox account

31. With the exception that I might store files on the 'Desktop' for the short-term, all electronic files (except for emails and temporary files) are stored by me on Dropbox. More information about the security arrangements of Dropbox can be found here: https://www.dropbox.com/en_GB/enterprise/security.

Files being accessed and/or accessible from my devices

32. Electronic files will never be opened on a screen in circumstances where they can be read by members of the public.

33. All of the electronic devices identified above will be kept secure at all times within the limits of reasonable practicability.

a. The phone and tablet are password protected and encrypted and will not be left unattended when away from home.

b. The laptop is encrypted using Microsoft BitLocker. It will only be left open and 'unlocked' where this is not reasonably avoidable or I am confident without doubt that the information on it will not be compromised (such as when it is left on my desk whilst I am temporarily elsewhere in chambers).

34. My laptop is protected by up to date anti-virus and anti-spyware software, subjected to regular virus scans and protected by an appropriate firewall.

35. Operating software is checked regularly to ensure that the latest security updates are downloaded.

36. Removable storage media such as memory sticks will be rarely used. I do sometimes accept documents on such media and rarely may load documents onto them. On such occasions the memory stick will be guarded as carefully as all other devices containing personal data.

Data Access

37. All data subjects have the right to access the information I holds about them, except where specific exemptions apply.

38. I will deal with subject access requests in accordance with the Subject Access Request Policy of No5 Chambers.

Disclosure

39. I may share data with other parties. The third parties with which I share data include—

- data processors, such as my Chambers staff, IT support staff, email providers, data storage providers
- other legal professionals
- witnesses
- courts and tribunals

- the staff in my chambers
- trainee barristers
- the members of Chambers who deal with complaints, the Bar Standards Board, and the Legal Ombudsman
- other regulatory authorities

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

Data Protection Training

41. I will ensure that I am appropriately trained in Data Protection.