GDPR Policy and Records of:

Alec Small

Albion Chambers
Broad Street
Bristol

BS1 1DR

ICO Reg: ZA028779

9 September 2022

Policy became operational on: 1 September 2022

Reviewed: 05 August 2024

Next review date: 05 August 2025

Contents

Contents 1
Data Protection Policy: 1
Mobile Working Policy 5
Data Breach Action Plan: 7
Near Miss Records: 8
Data Breach Records: 9
Information Processing: Reasons and Register: 10
Training Register: 12
IT Device Register: 13

Data Protection Policy:

Introduction:

1. As part of my role, I will regularly need to gather, be given and use personal data about a wide number of individuals. Be those clients, solicitors I work for, or other parties and individuals who are involved in cases, such as witnesses, defendants I prosecute etc.

2. I also need to manage data as part of my own practice management, not just for the provision of the services I offer. Such as committees at chambers, sifting pupillage applications, taking on mini-pupils etc. When I do so, I will be acting in my capacity as a data processor for chambers.

3. This policy, and attached documentation sets out how the data must be collated, stored and handled to meet my legal requirements.

How I get the information and why I have it:

4. Most of the personal information I process is provided to me directly by either government bodies, such as the CPS, or instructing solicitors for one of the following reasons:

    - The provision of legal advice to clients
    - Representation at legal proceedings of clients
    - As part of the prosecution of offences

5. Under the General Data Protection Regulation (GDPR), the lawful bases I rely on for processing this information are:

        a. Consent. Clients and others are able to remove their consent at any time. They can do this by contacting me at my business address above.
        b. I have a contractual obligation.
        c. I have a legal obligation.
        d. I have a vital interest.
        e. I need it to perform a public task.
        f. I have a legitimate interest.

What I do with the information I have:

6. I use the information that I have been given in order to:

    a. Provide solicitors and clients with legal advice and services.
    b. Prosecute offences on behalf of prosecuting authorities.
    c. Represent individuals at court and tribunal hearings.

7. I may share this information with:
    a. Professional colleagues for consultation and advice.

b. My professional regulatory bodies

c. Judicial bodies

d. Other organisations with consent.

Categories of Information I may hold:

8. All data my practice holds relating to identifiable individuals. This can include but is not limited to:
    - Name
    - Email address
    - Phone number
    - Address
    - Payment or bank details
    - Date of birth
    - Next of kin details
    - Details pertaining to education and employment
    - Information on your background & current circumstances
    - Financial information;

9. Special category personal data that reveals:

    - Racial or ethnic origin
    - Political opinions
    - Religious and philosophical beliefs
    - Trade union membership
    - Genetic data
    - Biometric data for the purpose of uniquely identifying a natural person
    - Data concerning health
    - Sex life and sexual orientation.

10. Personal information relating to individuals employed by an organisation, company or public body with whom I work is also included. As well as information which is held by prosecuting authorities in relation to the prosecution of offenders.

How I store information:

11. Information is securely stored at my business address, above. My personal address, on occasion, as well as remotely using electronic means.

12. I keep all information for a period of up to 7 years after our relationship has come to an end, so that I can respond to any complaints within the relevant time limits for such complaints to be brought. I will then dispose your information by shredding any paper documents, using a professional shredding service, as well as deleting any documents held electronically.

Data protection rights

13. Under data protection law, data owners have rights including:
    - Right of access - owners have the right to ask me for copies of their personal information.
    - Right to rectification - owners have the right to ask me to rectify information you think is inaccurate. They also have the right to ask me to complete information they think is incomplete.
    - Right to erasure - owners have the right to ask ne to erase their personal information in certain circumstances.
    - Right to restriction of processing - owners have the right to ask me to restrict the processing of their information in certain circumstances.
    - Right to object to processing - owners have the right to object to the processing of their personal data in certain circumstances.
    - Right to data portability - owners have the right to ask that I transfer the information they gave me to another organisation, or to them, in certain circumstances.
14. Data owners are not required to pay any charge for exercising their rights. If they make a request, I have one month to respond to them.

15. Please contact me at Alec Small, Albion Chambers, Broad Street, Bristol, (alec.small@albionchambers.co.uk, 0117 927 2144) if you wish to make a request.

Breaches:

16. In the event of a data breach: "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." I will:

    a. Instigate an investigation into the causes, and follow the actions in the action plan set out below.
    b. Report the breach, as necessary, to the ICO, within 72 hours of becoming aware of the breach at the latest.
    c. Assess whether I need to also report the breach to the Bar Standards Board.

Training:

17. Regular training and policy updates will be undertaken annually, and registered.

Retention and Disposal:

18. Unless a record, or datum has been marked for permanent preservation, it will only be retained for a minimum period. This will in most cases be a period of 7 years, however, other time limits may apply depending on a variety of factors such as:

    a. Practice needs
    b. Legislative requirements
    c. Complaint responses
    d. Defending or taking legal action

e. As is required by other agreements set by other data controllers.

19. Files in relation to Court of Protection cases may need to be held for longer, where the client lacks capacity.

20. When a case concludes, I will arrange and dispose of the papers in the following ways:

    a. First, all paper documents relating to the case which are not originals will be destroyed using the Chambers shredding services. Most, if not all of the documents I deal with are copies of electronically held documents, which are preserved using the Chambers Dropbox system, therefore, the originals are not required.
    b. I will then remove my direct access to the Dropbox for that case from my personal devices, access will then be retained by the Dropbox administrator and provided on request. (This reduces the potential scale of any data breaches if a device is lost or stolen.)
    c. Original documents will be returned to the original source, or, if consent is given, destroyed.
    d. Counsel's notebooks, when full, will be stored at chambers for the relevant period.
    e. Emails will be kept online for a period of 7 years, then wiped in line with Advanced practices.
    f. Dropbox folders will be wiped, when their expiry period is up.

21. Some pleadings may be retained in an anonymised form beyond the 6 year expiry date, for re-use in other cases.

22. No destruction will take place without it being clear that:

    a. The record is no longer required
    b. No work is outstanding
    c. No litigation, investigation or complaint is outstanding in relation to it.
    d. There are no current subject access request pending which affect it.

How to complain

23. You can also complain to the ICO if you are unhappy with how I have used your data.

24. The ICO's address:

    Information Commissioner's Office

    Wycliffe House

    Water Lane

    Wilmslow

    Cheshire

    SK9 5AF

    Helpline number: 0303 123 1113

Mobile Working Policy

This policy applies to my practice as a barrister and all personnel employed within the practice who remove case files, papers or other personal data from the precincts of chambers/office for the purposes of work.

Removing files:

It is strictly prohibited to remove client files or data from chambers or my home office for any other reason than carrying out legitimate activities in connection with my practice.

1. All files, case papers or notebooks leaving the office are to be stored in an appropriately secured bag, e.g. a suitcase – which has a lock or, for smaller items, a secure folder.
2. All items used to carry case papers should have this notice clearly displayed:

   "This belongs to Alec Small. If found please contact me urgently on 07708 484496 or please return to Albion Chambers, Broad Street, Bristol, BS1 1DR. This is a secure folder, which may contain confidential information. Any interference with the material or attempts to access it is strictly prohibited."

3. Case files or papers will not be left freely available in any common area where they may be read by other individuals, e.g. in public areas of courts, in coffee shops, on public transport or at hotels.
4. Case files will not be left in a position where another person entering the room or looking through a window might read them inadvertently.
5. Case files will not be read or worked on in public, such as on public transport or in coffee shops, in places where they can be overlooked by members of the public, including working on phones or laptops.
6. Case files can be worked on at home, provided that the material is put away in an opaque container when not in use. There will be appropriate physical security measures in place where any files are stored, for example the use of burglar alarms or a lock on the room the files are in.
7. All case files will be moved securely. On public transport case files should not be left unattended. If travelling by private car the files will be kept out of sight and stored as inconspicuously as possible, preferably in the boot. Case files should not be left in a car unattended except where the risk is less of a risk than taking it with you, such as when paying for fuel. It should never be left in a car overnight. If travelling by aeroplane, case files should be locked away in a suitcase with a lock on it, where possible kept as cabin luggage and should never be left unattended.
8. Do not dispose of hard copy papers that contain any client data outside chambers, including handwritten notes, Post-It notes etc.

Electronic devices:

This policy is applicable to all work and private devices which are used for professional purposes.

1. If you access emails from your mobile telephone you must ensure that the device is suitably password-protected.

2. Computers or devices must not be placed so that their screens can be overlooked, especially when working in co-working areas or public places.
3. Extreme care should be taken to ensure that laptops, removable devices and removable storage media containing client data are not lost or stolen. In particular:
    a. such laptops and other removable devices should never be left unattended in public places or left in a car overnight.
    b. the material on any laptop or other removable device should be kept to the **minimum amount** necessary to enable work to be carried out efficiently.
4. The electronic storage of case files requires certain minimum levels of security.
5. 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 an appropriate firewall for the computer used.
6. The operating software must be checked regularly to ensure that the latest security updates are downloaded.
7. Access to all computers must be password protected.
8. Particular care must be taken to avoid potential infection by malware, e.g. by downloading software from a source other than those which are trusted.
9. Work-in-progress should be regularly backed up, and backup media used for case files should be locked away securely.
10. Computers used for working on case files at home should be protected from unauthorised and unrestricted access by third parties, including family members. Where practicable, the ideal is a computer used only for work of the practice.
11. Work related documentation should not be stored solely on the hard-drive of any device. All work-related documentation should be saved within the Chambers' Drop-Box suite so that it can be deleted remotely in the event of a device being either lost or stolen. Regular checks should be undertaken to ensure that 'Downloads' folders are clear, and that work has not saved to the hard-drive incorrectly.

Data Breach Action Plan:

Note: The deadline for reporting a data breach to the ICO is 72 hours following notice of the breach.

Immediate Actions:

1. Identify nature of breach. (Is it physical paper missing, or is it a device containing electronic data?
2. Identify location of breach (where possible, where did you last have the data?)
3. Mitigate breach:
    a. Utilise Windows/Android services to remotely lock any devices
    b. Utilise OneDrive/Dropbox to remotely delete any documents from the missing device.
    c. Revoke device permissions remotely to use services where possible.
    d. Change all passwords to prevent device accessing sensitive services. (Microsoft, Dropbox, Chambers email, MLC, Google account, Bader, home Wi-Fi, banking etc.)
4. Identify what has been lost or accessed and whose data it is.
    a. Notify the parties and any instructing solicitors.
    b. Seek advice from Chambers.
5. Any other Actions?
6. Record details of the breach
    a. What was lost/breached?
    b. How?
    c. When?
    d. Who?
        i. Who is affected now?
        ii. Who else may be affected?
7. Evaluate: What could be done better in the future, can steps be put in place to prevent the issue re-occurring?

Notification List:

In the event of a breach, inform the following people:

1. Paul Fletcher, Chambers Director
2. Jessica Armfelt, Chambers Manager (particularly for IT queries and issues, as she can speak to Advanced)
3. Relevant clerk
4. Instructing Solicitor(s)
5. Individual subjects (if not contacted by Instructing Solicitor, above.)
6. Police (101 to report losses, 999 if an emergency)
7. Bar Standards Board
8. ICO
9. Indemnity insurers

Near Miss Records:

Date:	What Happened?	Who was involved/Affected?	What did you do in response?	Reportable? (Yes/No)	If not reported, why not?	Lessons Learned?

Data Breach Records:

Date:	What happened?	Who was involved/Affected?	What was done in response?	Consequences?	Who was informed?	Date of ICO notification	ICO response	Remedial Actions?

Information Processing: Reasons and Register:

Whose information do I process?	What data do I process?	What is my legal basis for doing so?	If Legitimate Interest, what is it?	Special Category data?	Legal basis for special categories?	Condition for processing criminal data
Instructing Solicitors	Name, contact details	Legitimate Interests	Provision of Legal Services			
Clients	Name, contact details, addresses, criminal history, employment history, etc.	Legitimate Interests	Provision of Legal Advice and Representation	Health data, nationality, criminal data,	processing is necessary for the establishment, exercise or defence of legal claims	In connection with, any legal proceedings; establishing, exercising or defending legal rights
Individuals related to cases, who I do not represent. (Witnesses, defendants I prosecute etc.)	Addresses, contact details,	Legitimate Interests	Provision of Legal Services	Health data, nationality, criminal data	processing is necessary for the establishment, exercise or defence of legal claims	In connection with, any legal proceedings; establishing, exercising or defending legal rights
Clerks/Staff	Name, Contact details	Legitimate Interests	Provision of Legal Services			
Other barristers	Name, Contact details, addresses	Legitimate Interests/Consent	Provision of Legal Services, talking to opponents and colleagues			

Pupils	Name, Contact details	Legitimate Interests/Consent	Provision of Legal Services, training lawyers			
Mini-Pupils	Name, contact details	Consent				

Training Register:

Date	Training undertaken	Provider	Grade?	Refresher Training by?
23.02.2021	Policy drafting and study of underlying guidance and requirements	Self-study, utilising ICO website, BSB website, Bar Council Website.	NA	28.02.22

IT Device Register:

Device/Service?	Provider	Description	Users	Serial No.	Encrypted?	Antivirus	Firewall?	Update?
Mobile Phone	Self	Nokia 9	Me	AOPGA1I931801022	Yes, phone	NA	NA	Auto
Laptop	Self	Surface Pro 3	Me	018726466953	Yes, EFS	Windows Defender	Yes	Auto
Laptop	Self	Surface Laptop	Me	004619100757	Yes, EFS	Windows Defender	Yes	Auto
Email	Chambers	Advanced/Microsoft	Me	NA				
Document Storage	Chambers	Dropbox	Me	NA				
Document Storage	self	OneDrive	Me	NA				