Data Protection Complaints Policy

1. Purpose

This Policy sets out how 8 New Square Chambers manages and responds to data protection complaints from data subjects in accordance with s.164A of the Data Protection Act 2018.

Its purpose is to ensure that we:

- comply with the statutory right of data subjects to complain regarding our processing of their personal data;
- provide a clear, accessible and consistent route for individuals to raise concerns about how we handle their personal data; and
- enable us to identify and put right any issues quickly, without the need for regulatory intervention.

2. Scope

This Policy applies to:

1. All personal data processed by chambers as a Data Controller under UK GDPR and the Data Protection Act 2018;
2. Complaints made by, or on behalf of, any individual whose personal data process, including, service users, employees, workers, job applicants, visitors, suppliers' staff, members of the public and children;
3. Processors and other suppliers acting on our behalf, to the extent set out in their contracts with us.

3. What is a Data Protection Complaint?

A data protection complaint encompasses any expression of dissatisfaction (however made, and whether or not framed in legal terms) about how the business or a specific individual has handled an individual's personal data, where the complainant considers that we have adversely affected their data protection rights or otherwise infringed the UK GDPR or Data Protection Act 2018.

Examples include dissatisfaction with how we have responded to a rights request, the security measures applied to personal data, a data breach, or how we have collected, used, shared or retained personal data.

A distinction should be made between complaints which relate to service and complaints which relate to data protection. We will not consider an expression of dissatisfaction about a service, or other matter that happens to be raised while exercising a data protection right (for example, the behaviour of a member of staff when accepting or responding to a SAR) under this policy. Such matters will be handled under our general complaints procedure, but the data protection elements will be dealt with under this Policy.

4. How individuals can make a data protection complaint

A complaint does not need to use legal terminology or mention the DUAA or UK GDPR to be treated as a data protection complaint, however complainants will be encouraged to use the following channels for raising a complaint.

Channels

Individuals can make a data protection complaint to us by any of the following channels:

1. By email to Harri Gibson harri.gibson@8newsquare.co.uk Data Protection Lead;
2. Post to the Data Protection Lead,
   Harri Gibson
   8 New Square Chambers
   8 New Square
   Lincoln's Inn
   London
   WC2A 3QP
3. Telephone on 020 7405 4321, where our team will take down the complaint in writing;
4. in person at our premises (staff will record the complaint and pass it to the DPM); and

We accept complaints however they reach us. A complaint will still be valid even if the complainant does not use one of the channels above, and staff will escalate it to the DPM.

Accessibility and reasonable adjustments

The complaints process is designed to be accessible to all individuals. We will make reasonable adjustments to enable people with disabilities, additional needs or language needs to complain, including by:

- Providing information about the process in plain English and, on request, alternative formats (for example large print, easy read or translated where possible);
- Accepting complaints from third parties acting on behalf of the data subject where authority is demonstrated; and
- Taking account of the best interests of children and other vulnerable individuals when designing responses.

Informing individuals of their right to complain

We will tell individuals that they can complain directly to us, as well as to the ICO, by including that information in our privacy notices (including the privacy notice on our website, staff privacy notice, and any product- or service-specific notices), both where data is collected directly from the individual and where it is obtained from a third party;

A dedicated complaints notice will also be maintained on 8 New Square's website. This describes the procedure, expected timeframes and the information we may need (for example proof of identity).

5. Receiving, logging and acknowledging complaints

Recognising a complaint

All staff are responsible for recognising a data protection complaint, even where it arrives through a non-standard channel (for example a service email inbox, social media mention or a conversation with a frontline colleague). If in doubt, staff must treat the matter as a potential data protection complaint and escalate it to the relevant DP Lead.

Logging

All data protection complaints must be logged on the Complaints Register maintained by the DPM, including:

- the date and channel of receipt;
- the complainant's details and their relationship with the Organisation;
- a summary of the complaint and the personal data / rights engaged;
- the date of acknowledgement, expected outcome date and any revisions;
- investigation notes, decisions and justification for the level of enquiries made;
- the outcome communicated, any remedial action and any referral to the ICO; and
- the closure date and lessons learned.

Acknowledgement within 30 days

We will acknowledge receipt of every data protection complaint in writing within 30 days of receipt, as required by s.164A(3) DPA 2018. In practice we aim to acknowledge within 5 working days.

Verifying identity and authority

Before responding we will verify the complainant's identity only where it is necessary and proportionate (for example where there is a real risk of disclosing personal data to the wrong person).

Where a complaint is made by a third party, we will request evidence of authority to act on the complainant's behalf.

6. Investigation and keeping the complainant informed

Proportionate investigation

We will take appropriate steps to respond to each complaint, including making reasonable enquiries, as required by s.164A(5)(a) DPA 2018. The scope of the investigation will be proportionate to the nature and seriousness of the complaint, the volume of personal data involved and any harm (or risk of harm) to the complainant.

Who investigates

For complaints relating to chambers processing, these will be investigated by the chambers Data Protection Lead. Where the complaint concerns a specific member of chambers, the complaint should be passed to that member for their own investigation.

Interaction with other processes

The complaint handler will consider whether the complaint also engages:

a) a personal data breach (in which case our Personal Data Breach Response Plan is triggered and we will consider notification to the ICO and to affected individuals where necessary);

b) an outstanding data subject rights request (handled under our Data Subject Rights Request Procedure, with the relevant statutory time limits);

c) a whistleblowing disclosure, safeguarding concern or employment grievance (handled under the relevant policy, in parallel where appropriate); or

Keeping the complainant informed

We will keep the complainant reasonably informed of progress, including the expected timeframe for a substantive response and any revisions, any information or evidence we need from them, and any material delays and the reasons for them.

Response timescales

We will respond to each complaint without undue delay. Consistent with ICO guidance, we aim to provide an outcome within three months of receipt at the latest. Where a complaint is straightforward, we will respond sooner. Where exceptional circumstances apply (for example a complex multi-jurisdictional matter or a matter involving large volumes of records), we will notify the complainant of the revised timeframe and the reasons.

7. Outcome and closure

Informing the complainant of the outcome

Once our enquiries are complete, we will tell the complainant the outcome of their complaint without undue delay, as required by s.164A(5)(b) DPA 2018. Our outcome response will be in writing, in plain and accessible language, and will:

1. summarise the complaint as we understood it;
2. set out the enquiries we made and the findings reached;
3. explain whether we consider there has been an infringement of data protection legislation and, if so, the nature of that infringement;
4. describe any action we have taken, or will take, to remedy the complaint (for example erasing or correcting personal data, updating processes or training, or providing an apology); and
5. remind the complainant of their right to complain to the Information Commissioner's Office, including contact details and a link to ico.org.uk.

Internal escalation

If the complainant is dissatisfied with the outcome, they may ask for an internal review of the decision by a senior member of the Chambers Management Committee. The review will be concluded without undue delay and ordinarily within 30 days.

Right to complain to the ICO

Complainants are entitled to complain to the ICO at any time, whether or not they have used this process, and whether or not they agree with our outcome. Please note, however, that the ICO will not ordinarily deal with complainants who have not first sought to address their complaint with chambers in the first instance.

The ICO can be contacted at **casework@ico.org.uk**

8. Record-Keeping

Personal data collected in handling a complaint is itself personal data and is processed under this Policy. We will retain complaint records for 7 years from closure of the complaint, in line with our Retention & Disposal Policy, and then securely dispose of them.

9. Monitoring, reporting and continuous improvement

The Data Protection Lead must:

- Maintain management information on complaints volumes, themes, timeliness and outcomes.
- report regularly to the Management Committee on complaints performance and any systemic issues identified.

- Use the collated complaints data to identify and drive improvements, including updates to privacy notices, contracts, processes and training;
- Review this Policy at least annually and in response to material changes in law, ICO guidance or our processing; and
- Be ready to comply with any future requirement made under s.164B DPA 2018 to report complaints volumes to the ICO, by capturing the relevant categorisation from the outset.

10. Processors, joint controllers and group companies

Where we engage a processor or share controllership with another organisation, we will require processors, through written contracts, to notify us promptly of any complaints they receive about personal data processed on our behalf, and to co-operate in our handling of them.