CITADEL CHAMBERS

DATA PROTECTION BREACH REPORTING PROCEDURE

As a Chambers, we are responsible for ensuring that personal data processed by the Chambers is not:

1 Accessed without authority;
2 Processed unlawfully;
3 Lost;
4 Destroyed; or
5 Damaged.

Nevertheless, we realise that from time-to-time things may go wrong and we might fail to achieve one or more of our data protection responsibilities. If this does happen, it is essential that we take steps to try to put things right. However, we can do this only if we know that there has been a problem. Therefore, everybody within Chambers has a duty to report any actual or suspected data breach, regardless of whether they have discovered the breaches or have caused them.

WHAT IS A DATA PROTECTION BREACH?

A data protection 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."
Data protection breaches can happen for a wide range of reasons, including:

1 Human error;
2 Cyber-attacks;
3 Loss or theft of devices or equipment on which personal data is stored;
4 Inadequate or inappropriate access controls;
5 Deceit; and
6 Disasters at Chambers' premises, for example, fire or flood.

If you are unsure whether a particular circumstance or incident constitutes a data protection breach, please refer the matter urgently to the Data Protection Manager (DPM) John Binks for guidance.

Reporting of data breaches by Barristers, Pupils and Staff

Although, as data controllers, Barristers are under no regulatory obligation to report a breach to Chambers, and are responsible individually for compliance with the notification and reporting obligations of the GDPR, nonetheless, Chambers recognises the role undertaken by Chambers as a Data Processor and acknowledges an obligation to support Data Controllers in those cases where it is appropriate to do so. In the case of a data breach caused by a member of Chambers the Barrister is requested to report the breach to the DPM. Chambers in their capacity as data processor will support any Barristers reporting and managing data breaches.

REPORTING A PERSONAL DATA BREACH

All personal data breaches involving members pupils and staff of which any member pupil or staff becomes aware must be reported to the DPM, John Binks immediately upon discovery.

Reports should be made by email to the DPM. When making a report, please detail:

- the nature of the suspected breach (theft, loss, destruction)
- the nature of the data involved in the breach (sensitive, personal, commercial etc)
- the scope of the breach (single client, multiple client, internal data)
- a description of the events relating to the breach (overview of why the breach came about)
- any chambers staff, barristers and/or other parties involved
- when the breach occurred
- any other information]

Following the report the breach will be considered and assessed as set out in our policy for managing data protection breaches , an action plan will be put in place where necessary and executed by the DPM. The DPM will be responsible for informing any joint controllers (in particular instructing solicitors and CPS) of the breach and proposed response

John Binks
Chambers Director
Citadel Chambers