Cyber and Information Security Affirmation (the "Affirmation")

I. Introduction

This Affirmation has been agreed by the Law Society and Bar Council. It is intended to be used where an individual self-employed barrister (the "Barrister") is instructed by a professional client[1] (the "Professional Client") on behalf of a lay client (the "Lay Client"). The barrister may have been engaged on the Standard Contractual Terms for the Supply of Legal Services by Barristers to Authorised Persons 2020 (the "Standard Terms"),[2] or on other terms approved by Bar Mutual.

II. Cyber and information security obligations

The Professional Client is likely to be subject to professional obligations concerning the confidentiality of the Lay Client's affairs. A solicitor or Solicitors Regulation Authority (SRA) regulated entity is, for example, professionally obliged by the SRA Code of Conduct for Solicitors, RELs (registered European lawyers) and RFLs (registered foreign lawyers),[3] to ensure that the service they provide to a client is competent and delivered in a timely manner (para 3.2), to maintain their competence to carry out their role and keep their professional knowledge and skills up to date (para 3.3), and to keep the affairs of current and former clients confidential unless disclosure is required or permitted by law or the client consents. (para 6.3).

The Barrister is subject to the Code of Conduct set out in the BSB Handbook,[4] and amongst other things has professional duties to act in the best interests of each client (CD2), to provide a competent standard of work and service to each client (CD7) and to keep the affairs of each client confidential (CD6). The Barrister must protect the confidentiality of the client's affairs, except for such disclosures as are required or permitted by law or to which their client gives informed consent (rC15.5).

In addition, each of the Professional Client and the Barrister are distinct[5] data controllers for the purposes of the UK General Data Protection Regulation (Regulation (EU) 2016/679 as retained in UK law) (the "Regulation") and Data

Protection Act 2018 (the "Act"), and is bound by the Regulation and the Act amongst other things, to implement appropriate technical and organisational measures to ensure an appropriate level of security of personal data including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

The terms on which the Barrister is engaged may contain other obligations concerning the use of technology, cybersecurity, data protection and other related matters.

III. Status

This Affirmation is not contractually binding and is of no legal effect, and nothing in this Affirmation varies, supplements or otherwise affects any terms on which the Professional Client engages the Barrister, or gives rise to or affects any professional or other duty or obligation of the Professional Client or the Barrister. It is not "guidance" for the purposes of the BSB Handbook I6.4. Instead, it is intended to underline some appropriate cyber and information security processes.

IV. Affirmation

Accordingly, given their legal and professional obligations, each of the Professional Client and the Barrister affirms that they intend:

- to be separate data controllers and not joint controllers, and that each be individually and separately responsible for complying with the legal and professional obligations that may apply to them;

- to process personal data in a manner that ensures appropriate security of that personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures,[6] which take into account (amongst other things) the state of the art, the nature, scope, context and purposes of processing, and the relevant risks (e.g. emerging cyber risks);[7]

- to consider that additional or different security measures may be required for the processing of special category information, such as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic or

biometric data concerning health or data concerning a natural person's sex life or sexual orientation;[8]

- to apply similar security measures to non-personal data as to personal data, and to bear in mind matters such as the intellectual property rights in, and the commercial and other sensitivity of such data;

- that they will each consider, and to the extent appropriate discuss between themselves, the use of technologies available to them to facilitate the secure transfer between them of personal and non-personal data;

- to notify the other without undue delay (ideally within 48 hours) of any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal or non-personal data transmitted, stored or otherwise processed,[9] to keep the other informed of all relevant developments in connection with the breach, and to take reasonable and proportionate steps to remedy or mitigate its effects;

- that each be responsible for ensuring that they have undertaken appropriate training to understand threats affecting the confidentiality, integrity, availability and resilience of personal and non-personal data;

- that any system used by them for the processing of personal and non-personal data will provide appropriate technical and organisational security measures to protect the information.

V. Notes

[1] An "Authorised Person" for the purposes of section 18(1)(a) of the Legal Services Act 2007, most frequently a solicitor.

[2] https://www.barcouncilethics.co.uk/documents/contractual-terms/

[3] https://www.sra.org.uk/solicitors/standards-regulations/code-conduct-solicitors/

[4] https://www.barstandardsboard.org.uk/for-barristers/bsb-handbook-and-code-guidance/the-bsb-handbook.html

[5] Other than in exceptional circumstances, a Barrister and those instructing them are not joint controllers of personal data within UK GDPR Art 26 (https://www.barcouncilethics.co.uk/wp-content/uploads/2022/10/Joint-data-controllers-under-the-GDPR-October-2022.pdf) nor are self-employed Barristers data processors within UK GDPR Art 28 (https://www.barcouncilethics.co.uk/documents/signing-controller-processor-agreements-with-solicitors-firms/)

[6] UK GDPR Art 5.1(f)

[7] UK GDPR Art 32.1

[8] UK GDPR Art 9

[9] cf UK GDPR Arts 4(12), 33 and 34

Version: 1, published 10 May 2024