**Processor record of processing carried out on behalf of a controller (Article 30(2) GDPR)**

Information about processor

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Name of processor | Contact details of processor | Processor’s representative | Contact details of processor’s representative | Processor’s data protection officer, if applicable | Contact details of processor’s data protection officer, if applicable |
| [Law Firm] | [Law firm contact details] | [Law firm representative for data protection matters] | [Contact details of law firm representative] |  |  |

Information about controllers

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| # | Name of controller | Contact details of controller | Controller’s representative | Contact details of controller’s representative | Controller’s data protection officer | Contact details of controller’s data protection officer |
| 1. |  |  |  |  |  |  |
| 2. |  |  |  |  |  |  |

Categories of processing carried out on behalf of each controller

1. Processing for the purpose of providing legal advice
2. Processing for the purpose of, or in connection with, legal claims, prospective legal claims, legal proceeding or prospective legal proceedings
3. Processing for the purpose of establishing exercising or defending legal rights
4. [other]

Transfers to third countries or international organisations, including the transfer mechanism safeguards

|  |  |  |
| --- | --- | --- |
| Personal Data | Destination Country/International Organisation | Transfer Mechanism Safeguards |
| Personal data on practice management system | Canada | Adequacy determination (Article 45 GDPR) |
| Personal data relating to file of controller 2 to [US lawyer] for the purpose of defending US legal claim | US | Derogation – Transfer necessary for the establishment, exercise or defence of legal claims (Article 49 (e) GDPR) |
| [additional transfers] |  |  |

Where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

1. All files stored on secure practice management solution
2. All staff use encrypted laptops
3. Access controls related to client files
4. Hard copy files stored in locked cabinet
5. [other]