



Ministry
of Justice

Data Sharing Memorandum of Understanding

THIS MEMORANDUM OF UNDERSTANDING (MoU) is made on the 5th June 2024

BETWEEN

THE SECRETARY OF STATE FOR JUSTICE of 102 Petty France, London SW1H 9AJ. Ministry of Justice (MoJ) Represented by The Office of the Public Guardian (OPG) of PO Box 16182, Birmingham B2 2WH.

AND

The Solicitors Regulation Authority (SRA) The Cube, 199 Wharfside Street, Birmingham, B1 1RN or DX 720293 BIRMINGHAM 47

GLOSSARY

In this MoU the following words and phrases will have the following meanings, unless expressly stated to the contrary

Definition	Interpretation
Criminal Offence Data	Criminal offence data includes the type of data about criminal allegations, proceedings, or convictions.
Data	Includes personal data, special category data and non-personal data that is collected for a legitimate business function by the Participants and when shared between the Participants can support the Participants to better deliver their respective business objectives and/or functions.
Data Protection Legislation	<p>(a) the UK General Data Protection Regulation (UK GDPR)</p> <p>(b) the Data Protection Act 2018 (DPA 2018)</p> <p>(c) The Privacy and Electronic Communications Regulations (PECR).</p>
Data Protection Impact Assessment (DPIA)	A tool that can be used to identify and reduce the privacy risks of any activity where Data is processed (including Data Sharing)
Data Subject	The identified identifiable living person to whom data relates (as defined in the Data Protection Legislation) See also Personal Data below.
General Data Regulation (GDPR)	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons regarding the processing of data and on the free movement of such data and repealing Directive 95/46/EC.
Human Rights Act 1998 (HRA)	Section 6, Human Rights Act 1998 (HRA) makes it unlawful for a public authority to act in a way that is incompatible with a person's rights under the European Convention on Human Rights. Section 6 imposes a duty on all public authorities to act compatibly with Convention rights.

1	INTRODUCTION AND PARTICIPANTS TO THE MoU
<p>1.1 This MoU will be entered into by the Office of the Public Guardian on behalf of the MoJ and the Solicitors Regulation Authority who are responsible for the purpose-specific data sharing activity to which this MoU relates.</p> <p>1.2 Office of the Public Guardian is an executive agency of the Ministry of Justice (MoJ) created in 2007 to support the Public Guardian in the discharge of his or her statutory functions.</p> <p>1.3 Collectively the bodies named above in section 1.1 are referred to as ‘participants’ and individually are referred to as a “participant”.</p>	
2	FORMALITIES
<p>2.1 This MoU will come into effect on 5th June 2024</p> <p>2.2 The date of the review of this MoU is 5th June 2027</p>	
3	CONTROLLER STATUS OF THE PARTICIPANTS
<p>3.1 The Office of the Public Guardian (OPG) and the Solicitors Regulation Authority (SRA) (“the participants”) are committed to working together to achieve the appropriate public interest outcomes in relation to solicitors who:</p> <ul style="list-style-type: none"> a. advise on or prepare Enduring or Lasting Powers of Attorney, b. exercise powers under those instruments, c. act as deputies appointed by the Court of Protection, d. act as guardians appointed by the High Court. <p>3.2 In support of the participants’ commitment to working together, this Memorandum of Understanding (MoU) sets out the framework for effective liaison, communication and information sharing between the participants.</p> <p>3.3 Each participant will act as the independent controller of their data.</p>	
4	TYPE OF DATA SHARING ACTIVITY
<p>4.1 The SRA will provide the OPG, so far as it is practicable and lawful to do so, and in accordance with the procedure set in this MoU, with indications or evidence (including but not limited to) of any misconduct on the part of a solicitor where it has reason to believe that the solicitor is acting as a Court of Protection appointed deputy or as a High Court appointed guardian or as an attorney under</p>	

	<p>a registered enduring or lasting power of attorney. This may include evidence of breaches or potential breaches of the civil law duties of a deputy, guardian or attorney.</p> <p>4.2 The OPG will, so far as it is practicable and lawful to do so, and in accordance with this MoU, pass to the SRA indications or evidence (including but not limited to) of professional misconduct on the part of a solicitor in the course of them acting as a Court of Protection appointed deputy, a High Court appointed guardian or as an attorney under a registered enduring or lasting power of attorney.</p>
5	PURPOSE AND INTENDED BENEFITS OF THE DATA SHARING
	<p>5.1 This section outlines compliance with the “Purpose Limitation” principle of the UK GDPR, and the second data protection principle of Part 2 of the Data Protection Act 2018 (DPA 2018).</p> <p><u>5.2 Purpose</u></p> <p>The aims of this MoU are to:</p> <ol style="list-style-type: none"> 1. assist both parties in their investigation or supervision work in the public interest so far as such assistance is lawful. 2. establish clear channels of communication between the participants. 3. promote a clear understanding of the SRA and OPG investigative processes, relevant legislation, working procedures and legal constraints. 4. enable both the SRA and the OPG to co-operate operationally. 5. facilitate effective investigation and the lawful exchange of information between the participants to further the respective organisations’ aims in protecting vulnerable people and those accessing legal services. <p>5.3 The OPG and the SRA recognise and respect their differing statutory duties, operational priorities and constraints, and confidentiality requirements. However, in the public interest, they commit themselves to professional co-operation in preventing or acting in relation to the suspected abuse of vulnerable adults involving law firms or solicitors.</p>
6	LEGAL CONSIDERATIONS – ROLE OF THE OPG AND SRA - ITS POWERS
	<p><u>6.1 The Role of the OPG and its powers</u></p> <p>The post of the Public Guardian was created under section 57 of the Mental Capacity 2005 (“the Act”).</p>

The Act provides that the Public Guardian is to be supported by officers and staff, and this led to the creation of the Office of the Public Guardian (OPG).

The OPG supports the Public Guardian in the registration of enduring powers of attorney and lasting powers of attorney, the investigation of concerns relating to attorneys, guardians and deputies, and the supervision of deputies and guardians.

The OPG provides some general help to attorneys, guardians and deputies to carry out their duties and protects people who lack the mental capacity to make decisions for themselves, known as ("P").

The OPG's statutory powers derive from the Act and the Lasting Powers of Attorney, Enduring Powers of Attorney and Public Guardian Regulations 2007 ("the 2007 Regulations") and (Amendment) Regulations 2010 ("the 2010 Regulations") and The Guardianship (Missing Persons) Act 2017.

The powers include the supervision of Court of Protection appointed deputies and High Court appointed guardians, dealing with representations about the way in which a Court of Protection appointed deputy, High Court appointed guardian or attorney acting under a registered enduring or lasting power of attorney is exercising his or her powers.

The OPG's enquiry and regulatory powers are found in:

- Section 58 of the Act – 'Functions of the Public Guardian'
- Regulation 40, 41, 46, 47 of the 2007 Regulations
- Regulation 48 of the 2007 Regulations as amended by the 2010 Regulations.
- The Guardianship (Missing Persons) Act 2017

The Public Guardian may bring proceedings to either the Court of Protection or the High Court in connection with his or her functions.

6.2 The Role of the SRA and its powers

The SRA is a company (Solicitors Regulation Authority Limited) registered in England and Wales (company registration number 12608059) whose registered office is at the Cube, 199 Wharf side Street, Birmingham B1 1RN.

It is the independent regulatory body responsible for the regulation of legal services by law firms and solicitors in England & Wales.

The SRA's powers arise from various statutes and regulations including: -

- Solicitors Act 1974,
- Administration of Justice Act 1985,
- Courts and Legal Services Act 1990,
- Legal Services Act 2007 and
- SRA's Standards and Regulations.

The SRA investigates allegations of breaches of its requirements and where appropriate makes findings and imposes disciplinary sanctions.

The SRA has statutory and rule-based powers to require the production of documents or information, such as section 44B of the Solicitors Act 1974 and section 93 of the Legal Services Act 2007.

The SRA may inspect material that is subject to a law firm's client's legal professional privilege (LPP) or confidentiality but may only use such material for its regulatory purposes.

The SRA also protects the LPP and confidentiality of clients.

LPP material will not be disclosed by the SRA to any other person other than where necessary for its regulatory purposes.

Material that is not subject to LPP may be disclosable in the public interest, in the absolute discretion of the SRA, including material comprising communications in furtherance of crime or fraud.

The SRA can act on information from any source, including clients and members of the public, solicitors and firms, or organisations such as the OPG. Where it decides to investigate it may follow different approaches:

- a. a paper-based investigation which includes obtaining an explanation from the subject solicitor.
- b. investigation by attendance on solicitors' premises which includes the inspection of accounts and client files. These inspections may be undertaken without notice.
- c. a decision then to either close the investigation without further action or to take some form of action such as issuing a warning, a rebuke or a fine or imposing a condition on a solicitor's practising certificate. Most internal decisions made by the SRA are published on its website.

The investigation of serious misconduct, including dishonesty, may lead to two possible outcomes:

- a. Intervention – the SRA can effectively close a solicitor's practice where there is "reason to suspect dishonesty" by the solicitor or there are serious breaches of its standards and regulations. In deciding whether to intervene, a balance must be achieved between protection of the public and the interests of the solicitor. Failure to intervene may have serious consequences for clients, but the consequences of an intervention for solicitors are very serious also.
- b. Prosecution at a hearing heard in public before the Solicitors Disciplinary Tribunal by the SRA, in any case where it is likely that a solicitor would be subject to a suspension from practice or be struck off the Roll of Solicitors.

The SRA investigates and prosecutes breaches of Sections 20 to 24 of the Solicitors Act 1974 and Sections 14 to 17 of the Legal Services Act 2007.

These relate to offences committed by non-solicitors holding themselves out as solicitors, undertaking functions reserved for qualified solicitors or fraudulently obtaining employment in solicitors' offices as solicitors.

7	LEGAL CONSIDERATIONS – LEGAL POWERS TO SHARE DATA
----------	--

OPG

7.1 The OPG carries out its functions as governed by the Mental Capacity Act 2005, and the lawful basis for processing of personal data relating to those functions is that set out under Article 6 (1)(e) of the GDPR, namely that “the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller”.

The lawful basis for the processing of special category data by the OPG is generally that set out in Article 9(2)(g) of the GDPR – i.e., “processing is necessary for reasons of substantial public interest”.

SRA

7.2 The SRA is the independent regulatory body responsible for the regulation of legal services by law firms and solicitors in England and Wales. The SRA was formed in January 2007 by the Legal Services Act.

The SRA’s legal powers arise from various statutes and regulations including the Legal Services Act 2007, the Solicitors Act 1974, the Administration of Justice Act 1985, the Courts, and Legal Services Act 1990 and the SRA’s Standards and Regulations.

The SRA collect, use, and share data primarily in the exercise of its regulatory functions. The SRA’s lawful basis for processing this information is under UK GDPR is Article 6 Section 1(e) and Article 9 Section 2(g) as it is necessary for the exercise of official authority in the public interest.

8	FAIRNESS/TRANSPARENCY
----------	------------------------------

This section outlines compliance with the ‘**Fair & Transparent**’ aspects of the **Lawfulness, Fairness and Transparency** Principle of the UK GDPR, and the first data protection principle of the DPA 2018.

OPG

8.1

OPG states within its privacy notices for lasting and enduring powers of attorney, guardianship supervision and for deputyship supervision that data sometimes needs

to be shared with other organisations but where this is necessary it will comply with all aspects of the data protection laws.

Within its privacy notice for deputy supervision, OPG provides a non-exhaustive list of organisations with whom it may share data. This list includes the Solicitors Regulation Authority. Within its privacy notice for guardianship supervision, OPG provides a non-exhaustive list of organisations with whom it may share data. At the time of this agreement, this does not include the Solicitors Regulation Authority specifically but this is covered by it being stated as a non-exhaustive list.

Data subjects will not usually be directly notified when their data will be shared under these circumstances.

SRA

8.2

SRA states within its privacy notice that data will be shared with other law enforcement and regulatory bodies.

Data subjects will not usually be directly notified when their data will be shared under these arrangements as the restriction to this right will be applied.

9 THIRD-PARTY PROCESSING

OPG

9.1

All OPG data is hosted in both the UK and Ireland.

SRA

9.2

SRA has provided a link to their privacy notice: [SRA | Privacy notice | Solicitors Regulation Authority](#).

10 DATA PROTECTION IMPACT ASSESSMENT (DPIA)

10.1 The OPG will undertake to complete a DPIA in relation to this MoU after the agreement has been completed by the SRA, as this is a mandatory requirement by the MoJ on the OPG.

10.2 The SRA processing is not considered high risk and a DPIA is not required. Disclosures are dealt with on a case-by-case basis and any risks can be considered at that stage.

11	INFORMATION SHARING AND DATA PROTECTION
<p><u>11.1 Information sharing</u></p> <p>Where it is lawful and in the public interest to do so, the parties agree to disclose the necessary and relevant information to the other:</p> <p>a) to enable the assessment of risk to the public such as to:</p> <ol style="list-style-type: none"> i. Identify and minimise or remove any mismanagement of P's property and financial affairs by a solicitor acting as the deputy or attorney for P or as a guardian for a missing person; ii. protect vulnerable persons, namely 'P'; iii. minimise the risk of fraud or other criminality by a solicitor acting as the deputy or attorney for P or as a guardian for a missing person; <p>b) so that alleged criminality, misconduct, breaches of the SRA principles, or other failures are properly investigated and decided upon;</p> <p>c) to enable the proper processing of claims or applications for redress or compensation of any description; and</p> <p>d) for the purposes of regulatory, disciplinary, or other legal proceedings, whether in public or not;</p> <p>provided that the recipient is reasonably considered able to take regulatory or other proper action upon the information.</p> <p>The types of data that may be shared is Personal Data and Special Category Data and is classed as Data sharing non-commercial.</p> <p>The minimum amounts of data should be shared between the two organisations and should only be escalated to allow both organisations to complete their statutory roles.</p> <p><u>11.2 Data Protection</u></p> <p>The recipient of information received from the other party will:</p> <ul style="list-style-type: none"> • always comply with UK data protection legislation and any relevant codes of conduct or certifications. • keep the information secure. • use the information only for proper purposes, such as regulatory, disciplinary, or other legal investigations or proceedings; and • liaise or co-operate where appropriate to avoid action that prejudices or may prejudice an investigation by another party or person. 	

Proper purposes may also include further lawful disclosure of the information such as to persons under investigation, witnesses, legal advisers, other regulators, professional bodies, prosecuting bodies, and law enforcement agencies including the police, HM Revenue and Customs, the National Crime Agency (or any body that in future carries out the functions of such bodies).

The parties agree to ensure that disclosures to the other party are lawful including the common law principles of confidentiality and privacy and the Human Rights Act 1998.

The disclosing party also agrees to notify the recipient of:

- a. any restrictions on the use to which the information can be put, and
- b. any restrictions which apply to the onward disclosure of the information, and

in the absence of such notification, the receiving party may assume that there are no such restrictions (in addition to any restrictions that apply as a matter of law).

12. EXCHANGE OF DATA

12.1 All information requests and information exchanged between the parties should be passed via the nominated Points of Contact (POC) as nominated below -

- **The SRA's Intelligence Manager**
- **OPG's Operational Delivery Manager (Investigations)**
- **OPG's Operational Delivery Manager (Supervision)**
and/or
- **OPG's Head of Information Assurance**

Both organisational bodies should endeavour to provide a dedicated email address to facilitate this function, which is reviewed and responded to within 48 hours to support each bodies functions and actions.

All correspondence will be between these persons, their respective nominees or otherwise by arrangement and this may include those working on a particular file.

The SRA and OPG SPOCs may change from time to time. The parties will notify each other in writing of any such change.

When the SRA receives evidence of an allegation of fraud or other criminal activity by a solicitor in relation to a deputyship, guardianship, enduring power of attorney or lasting power of attorney, a representative will in appropriate cases notify OPG's representative as soon as practicable by email, and where appropriate, before any overt action is taken.

When the OPG receives evidence of an allegation of fraud or other criminal activity by a solicitor, a representative will in appropriate cases notify SRA's representative as soon as practicable by email and, where appropriate, before any overt action is taken.

The parties can then consider the proper course of action having regard to their respective priorities and any requirement for confidentiality.

12.2 Service Levels

Both participants will endeavour to deal with requests for data within 7 days.

Where the nature of the request (for example because of the complexity or volume of information requested), is such that it has not been or cannot be dealt within 7 days, the participant dealing with the request will update the requesting participant with progress and an estimate as to when the request will be dealt with or with an explanation as to why the information cannot be provided.

If the request is urgent, then this will be highlighted by the participant making the request and an appropriate timescale for the processing of the request will be agreed.

12.3 Format

The data will be provided in a stand-alone MS word, excel or report format as per the request and what has been asked for.

There will be no access to each other's bespoke case management databases.

Compliance with the Accuracy Principle of the UK GDPR, and the fourth principle of Part 2 of the DPA 2018.

12.4 Accuracy of the shared data

The originating data sharing participant must ensure that the Personal Data and Special Category Data being shared has had all reasonable steps taken to ensure that it is both accurate and up to date in accordance with the Accuracy Principle.

All data to be shared must be checked by more than one person and at least one senior grade higher than the person compiling the work as part of the request.

12.5 Notification of errors in the data/Information shared.

The disclosing participant will notify the receiving participant of any errors within one working day of discovery to the nominated SPOC.

12.6 Rectification

If an error is found this will be rectified as soon as practicable depending on the size and nature of the original request.

13 DATA SECURITY

Compliance with the **Integrity and Confidentiality** Principle of the UK GDPR, and the sixth data protection principle of the DPA 2018.

13.1 Security Standards

The SRA applies all the controls in the ISO:27001 standard.

The OPG complies with relevant HMG guidance - the SPF contains subsidiary guidance in the more recent GOV standards - for example, GOV007 for security [Government security - GOV.UK \(www.gov.uk\)](http://www.gov.uk)

Government security - This series brings together all documents relating to government security.

Functional Standards - A suite of management standards and associated documentation to guide people working in and with the UK government. You can see all the functional standards here [Functional Standards - GOV.UK \(www.gov.uk\)](http://www.gov.uk)

13.2 Security and assurance

The Participants agree to:

- a. only provide the necessary and relevant data
- b. only use the data for the purposes for which they have received it.
- c. transfer data securely through a password protected format.
- d. store data securely
- e. ensure that only people who have a genuine business need to see the data will have access to it.
- f. report data losses or wrongful disclosure to each participant's designated data protection officer
- g. only hold the data while there is a business need to keep it and in accordance with data protection legislation.
- h. destroy it in line with retention policies.

- i. seek approval from the originating participant for any onward disclosure.
- j. each provide assurance that they have complied with these principles, upon request.

14		DATA SUBJECT RIGHTS		
14.1				
Data Subject Right	Data Processing Regime: i.e., Part 2 of the DPA or Part 3 of the DPA	Applies to MoJ/OPG Y/N	Applies to SRA Y/N	If right does not apply provide reason why
Be Informed	<u>DPA Part 2 Article *(1) child consent</u>	<u>Y</u>	<u>N</u>	
Access	<u>Part 4, Chapter 3, Section 94</u>	<u>Y</u>	<u>Y</u>	
Rectification	<u>Part 3, Chapter 3 section 46</u>	<u>Y</u>	<u>Y</u>	
Erasure	<u>Part 3, Chapter 3, Section 47</u>	<u>Y</u>	<u>N</u>	<u>Does apply to public task</u>
Restriction		<u>N</u>	<u>N</u>	
Portability		<u>N</u>	<u>N</u>	
Object	<u>Part 4, Chapter 3, section 99</u>	<u>Y</u>	<u>N</u>	This does not apply to SRA
Automated decision-making and profiling		<u>N</u>	<u>N</u>	
<p>14.2 In the event that a data subject right request relating to the personal data shared under this MoU is received by either participant, the participants will individually consult with each other on the proposed response and respond to the request in accordance with Data Protection Legislation, and in accordance with their respective organisation's internal procedures for responding to data subject access right requests.</p> <p>14.3 Where a request is received to rectify, erase, or restrict any personal data shared under this MoU, the receiving Participant will communicate any rectification or</p>				

erasure of personal data or restriction of processing carried out in accordance with Data Protection Legislation to the other Participant.

14.4 The contacts for consulting and responding to data subject access right requests for the participants are the nominated SPOCs, the details of which are provided at section 12 of this MOU.

15	FREEDOM OF INFORMATION ACT (FOI) REQUESTS
-----------	--

15.1 The participants will assist and co-operate with each other to enable each organisation to comply with their information disclosure obligations.

15.2 In the event of one participant receiving an FOI access request that involves disclosing information that has been provided by the other participant, the participant in question will notify the other to allow it the opportunity to make representations on the potential impact of disclosure and will issue a formal response following its internal procedures for responding to FOI requests within the statutory timescales.

15.3 The designated contact and nominated SPOCs for responding to FOI requests for the participants are provided at section 12 of this MoU.

16	RETENTION AND DESTRUCTION
-----------	----------------------------------

This section outlines compliance with the **Storage Limitation** principle of the UK GDPR and the fifth data protection principle under Part 3 of the DPA 2018.

16.1 Data will be retained by OPG in line with the MOJ/OPG published Record Retention & Disposition Schedule, which can be found at this link:

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/856593/opg-rrds.docx

16.2 OPG will apply secure destruction methods at the point of destruction, considering whether the information is in hard copy form or electronic and adhering to MoJ guidelines in place at that time.

16.3 SRA has provided a link to their Records Retention and Destruction policy - <https://www.sra.org.uk/globalassets/documents/sra/records/record-retention-schedule.pdf?version=48ed74>

17	COMPLAINTS HANDLING/DISPUTE RESOLUTION
-----------	---

17.1 Issues and problems that arise between the participants concerning the operation of this MoU will be resolved through discussion by the SPOCs listed at section 12, with escalation to more senior managers where necessary.

18	MONITORING AND REVIEWING ARRANGEMENTS
-----------	--

18.1 The MoU review process will focus on:

- whether the MoU is still necessary and fit for purpose
- whether the existing data sharing arrangements should be extended or amended
- whether the lawful bases relied upon by the participants for sharing the data remain valid, including whether any legislation has been amended or enacted that would impact on any purpose-specific information sharing activities. If a participant's lawful basis for information sharing has changed, the data sharing activity in place may need to be amended to reflect this.

18.2 In the event of a personal data breach or other breach of the terms of this MoU any of the participants, this MoU must be reviewed immediately by the participants.

18.3 A record of all reviews will be created and retained by each participant.

18.4 Reporting and review arrangements

The participants will use their best endeavours to review the operation of this MoU every three years. Any changes to this MoU must be agreed in writing.

19	COSTS AND LIABILITY
-----------	----------------------------

19.1 No costs/charges will be made.

19.2 Nothing in this MoU shall, or is intended to:

- a) create any legal or procedural right or obligation which is enforceable by either participant against the other; or
- b) create any legal or procedural right or obligation which is enforceable by any third party against either of the participants or against any other third party; or
- c) prevent either of the participants from complying with any law which applies to them; or
- d) fetter or restrict in any way whatsoever the exercise of any discretion which the law requires or allows the participants to exercise; or

- e) create any legislative expectation on the part of any person that either of the participants to this MoU will do any act (either at all, or in any particular way, or at any particular time) or will refrain from doing any act.

Nonetheless the participants are genuinely committed to pursuing the aims and purposes of this MoU in good faith and intend to act in accordance with its terms on a voluntary basis.

20	TERMINATION
-----------	--------------------

20.1 This MoU will remain in force until terminated by either participant. Either participant may terminate this MoU upon 2 (two) months written notice to the other participant, or after an agreed period.

20.2 Termination notices must be referred to the signatories of the MoU.

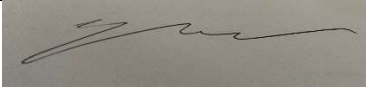

20.3 The participants will have the right to terminate this MoU should the following circumstances arise:

- a material breach by the other Participant of any of the terms of the MoU
- by reason of cost, resources, or other factors beyond the control of either of the participants
- if any material change in circumstances occurs which, following negotiation between the participants, in the reasonable opinion of either or all the Participants significantly impairs the value of the MoU in meeting their objectives.

20.4 It is recognised that there may be some circumstances (for example, see the situations listed below) where it may not be possible to terminate a data sharing activity. Should such circumstances arise, the participants must refer to the signatories of this MoU who will decide how the data sharing activity will be managed.

- the sharing of data is essential to the participants to provide their business service and termination of the MoU would severely impact the organisation's ability to fulfil their statutory obligations and
- the sharing of data is necessary to satisfy a legal requirement.

20.5 Where a decision is made to terminate this MoU the participants will consult with each other to determine how the data shared between the participants is handled.

21	DATA BREACHES / INFORMATION SECURITY BREACHES
<p>21.1 Personal data/information security breaches, including misuse of MoJ information or the OGD/External Organisation information shared under this MoU must be reported to the designated contacts/ SPOCs for each participant.</p> <p>21.2 The OPG and the SRA will deal with any information security breaches found within or made by their respective organisations and will follow the FOI, SAR, GDPR and Data Protection rules on security breaches following the rules and timescales imposed under those rules.</p>	
22	SIGNATORIES
<u>Transparency</u>	
This Agreement is a public document, and the parties may publish it as they separately see fit.	
Signed on behalf of the MoJ/OPG:	
22.1 I accept the terms of the Process Level Memorandum of Understanding on behalf of the MoJ.	
Signature:	
Name:	Peter Boyce
Position:	Deputy Director Legal and Information Assurance, and Senior Information Risk Owner
Date:	5 June 2024
Signed on behalf of the Solicitors Regulation Authority	
22.2 I accept the terms of the Process Level Memorandum of Understanding on behalf of the Solicitors Regulatory Authority	
Signature:	
Name:	Andrew Turton
Position:	Director of Risk and Information Governance
Date:	5 June 2024