

**DIGITAL SHADOWS DATA PROCESSING TERMS**  
(Effective 25 November 2022)

**BACKGROUND**

- 1 This Data Processing Agreement ("**DPA**") sets out the terms, requirements, and conditions on which Digital Shadows will process Personal Data when providing the SearchLight™ or other related services ("**Service**") to a user or customer ("**Customer**") pursuant to the use of the Service ("**Agreement**").
- 2 Any use or acceptance of any part of the Service, constitutes the Customer's acceptance of this DPA. If you do not agree to the terms of this DPA, do not proceed further nor continue use of any Service. Digital Shadows reserves the right to change the terms of this DPA at any time upon thirty (30) days' written notice by updating the DPA shown on the website. If the Customer objects to any changes then the Customer should cease using the Service. If the Customer continues to use the Service at the end of such thirty (30) day period, Customer will be deemed to have accepted the revised DPA.
- 3 This DPA contains the Standard Contractual Clauses for international transfers.

**AGREED TERMS**

**1 DEFINITIONS AND INTERPRETATION**

The following definitions and rules of interpretation apply in this DPA.

1.1 Definitions:

"**Addendum**" means as defined at Schedule 2.

"**Business Purposes**" means the Service to be provided by Digital Shadows to the Customer or any other purpose specifically identified in the Schedule.

"**CCPA**" means California Consumer Privacy Act of 2018, Cal. Civil Code § 1798.100 et seq. (as amended). As of January 1, 2023, CCPA shall mean the California Privacy Rights Act.

"**Controller**" and "**Processor**" are as defined in the Data Protection Legislation.

"**Data Protection Legislation**" means the European Union legislation relating to Personal Data, UK Data Protection Legislation, the CCPA and all other legislation and regulatory requirements in force from time to time which apply to a party relating to the use of Personal Data (including, without limitation, the privacy of electronic communications).

"**Data Subject**" means an individual who is the subject of Personal Data.

"**EU Standard Contractual Clauses**" means the standard contractual clauses for the transfer of personal data to third countries pursuant to the GDPR, adopted by the European Commission under Commission Decision (EU) 2021/914 including the text from module 2 of such clauses and no other modules and not including any clauses marked as optional in the clauses unless otherwise stated.

"**FADP**" means the Swiss Federal Act on Data Protection of 19 June 1992 and the revised version of 25 September 2020 when in force.

"**GDPR**" means mean Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

"**Personal Data**" means any information, including Personal Information, relating to an identified or identifiable natural person that is processed by Digital Shadows as a result of, or in connection with, the provision of the Service, an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

**DIGITAL SHADOWS DATA PROCESSING TERMS**  
(Effective 25 November 2022)

**“Personal Data Breach”** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, the Customer's Personal Data transmitted, stored or otherwise processed.

**“Personal Information”** has the meaning given to it in the CCPA.

**“Processing, processes and process”** means either any activity that involves the use of Personal Data or as the Data Protection Legislation may otherwise define processing, processes or process. It includes any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing also includes transferring Personal Data to third parties.

**“Standard Contractual Clauses”** means the EU Standard Contractual Clauses and the Addendum.

**“UK Data Protection Legislation”** means all applicable data protection and privacy legislation in force from time to time in the UK including the UK GDPR; the Data Protection Act 2018; the Privacy and Electronic Communications Directive 2002/58/EC (as updated by Directive 2009/136/EC) and the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426) as amended.

**“UK GDPR”** means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27th April 2016 on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data (General Data Protection Regulation) as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018.

- 1.2 The appendices form part of this DPA and will have effect as if set out in full in the body of this DPA. Any reference to this DPA includes the appendices.
- 1.3 A reference to writing or written includes email but not fax.
- 1.4 In the case of conflict or ambiguity between:
  - 1.4.1 any provision contained in the body of this DPA and any provision contained in the appendices, the provision in the body of this DPA will prevail; and
  - 1.4.2 any of the provisions of this DPA and any executed Standard Contractual Clauses, the provisions of the executed Standard Contractual Clauses will prevail.

## **2 PERSONAL DATA TYPES AND PROCESSING PURPOSES**

- 2.1 The Customer and Digital Shadows acknowledge that for the purpose of the Data Protection Legislation, the Customer is the Controller and Digital Shadows is the Processor.
- 2.2 The Customer retains control of the Personal Data and remains responsible for its compliance obligations under the applicable Data Protection Legislation, including providing any required notices and obtaining any required consents, and for the processing instructions it gives to Digital Shadows.
- 2.3 The Customer warrants and represents that Digital Shadows' expected use of the Personal Data for the Business Purposes and as specifically instructed by the Customer will comply with the Data Protection Legislation.
- 2.4 The Schedule describes the subject matter, duration, nature and purpose of processing and the Personal Data categories and Data Subject types in respect of which Digital Shadows may process to fulfil the Business Purposes of the Service.
- 2.5 Digital Shadows will not sell or exploit the Personal Data it is Processing for the Customer for profit with any third party.

**DIGITAL SHADOWS DATA PROCESSING TERMS**  
(Effective 25 November 2022)

**3 DIGITAL SHADOWS' OBLIGATIONS**

- 3.1 Digital Shadows will only process the Personal Data to the extent, and in such a manner, as is necessary for the Business Purposes in accordance with the Customer's written instructions. Digital Shadows will not process the Personal Data for any other purpose or in a way that does not comply with this DPA or the Data Protection Legislation. Digital Shadows will immediately notify the Customer if, in its opinion, the Customer's instruction would not comply with the Data Protection Legislation.
- 3.2 Digital Shadows will promptly comply with any Customer request or instruction requiring Digital Shadows to amend, transfer, delete or otherwise process the Personal Data, or to stop, mitigate or remedy any unauthorised processing.
- 3.3 Digital Shadows will maintain the confidentiality of all Personal Data and will not disclose Personal Data to third parties unless the Customer or this DPA specifically authorises the disclosure, or as required by law. If a law, court, regulator or supervisory authority requires Digital Shadows to process or disclose Personal Data, Digital Shadows will first use its reasonable endeavours to inform the Customer of the legal or regulatory requirement and give the Customer an opportunity to object or challenge the requirement, unless the law prohibits such notice.
- 3.4 Digital Shadows will reasonably assist the Customer with meeting the Customer's compliance obligations under the Data Protection Legislation, taking into account the nature of Digital Shadows' processing and the information available to Digital Shadows, including in relation to Data Subject rights, data protection impact assessments and reporting to and consulting with supervisory authorities under the Data Protection Legislation.
- 3.5 Digital Shadows will promptly notify the Customer of any changes to Data Protection Legislation that may adversely affect Digital Shadows' performance of the Service.
- 3.6 Customer acknowledges that Digital Shadows:
- 3.6.1 will add certain data discovered in the course of providing the Service (other than Personal Data it processes on the Customer's behalf) into its proprietary platform for the benefit of the Customer and Digital Shadows' other customers, and to the extent such data includes Personal Data, Digital Shadows is a Controller and this DPA does not apply to such Personal Data; and
  - 3.6.2 is free to use meta-data, statistics and such other information derived from the Personal Data it receives from Customer which cannot be identified as originating or deriving directly from such Personal Data, and cannot be reverse-engineered by a third party such that it can be so identified, for any purpose whatsoever.

**4 DIGITAL SHADOWS' EMPLOYEES**

- 4.1 Digital Shadows will ensure that all employees:
- 4.1.1 are informed of the confidential nature of the Personal Data and are bound by confidentiality obligations and use restrictions in respect of the Personal Data;
  - 4.1.2 have undertaken training on the Data Protection Legislation relating to handling Personal Data and how it applies to their particular duties; and
  - 4.1.3 are aware both of Digital Shadows' duties and their personal duties and obligations under the Data Protection Legislation and this DPA.

**5 SECURITY**

- 5.1 Digital Shadows will at all times implement appropriate technical and organisational measures against unauthorised or unlawful processing, access, disclosure, copying, modification, storage, reproduction, display or distribution of Personal Data, and against accidental or unlawful loss, destruction, alteration, disclosure or damage of Personal Data including, but not limited to, the security measures set out in the Schedule.

**DIGITAL SHADOWS DATA PROCESSING TERMS**  
(Effective 25 November 2022)

- 5.2 Digital Shadows may update the measures in the Schedule from time to time, provided they do not result in a reduction in the security over the Personal Data to which they apply. Digital Shadows will maintain an up to date written record of its then-current security measures, which it shall provide to the Customer on request, and review at least on an annual basis to ensure they remain current and complete.
- 5.3 Digital Shadows implements such measures to ensure a level of security appropriate to the risk involved, including as appropriate:
- 5.3.1 the pseudonymisation and encryption of Personal Data;
  - 5.3.2 the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
  - 5.3.3 the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and
  - 5.3.4 a process for regularly testing, assessing and evaluating the effectiveness of security measures.
- 6 PERSONAL DATA BREACH**
- 6.1 Digital Shadows will promptly and without undue delay notify the Customer if any of the Customer's Personal Data is lost or destroyed or becomes damaged, corrupted, or unusable. Digital Shadows will restore such Personal Data at its own expense.
- 6.2 Digital Shadows will without undue delay notify the Customer if it becomes aware of:
- 6.2.1 any accidental, unauthorised or unlawful processing of the Customer's Personal Data; or
  - 6.2.2 any Personal Data Breach relating to the Customer's Personal Data.
- 6.3 Where Digital Shadows becomes aware of an event within the scope of clause 6.2, it shall, without undue delay, also provide the Customer with the following information:
- 6.3.1 a description of the nature of such event, including the categories and approximate number of both Data Subjects and Personal Data records concerned;
  - 6.3.2 the likely consequences of the event; and
  - 6.3.3 a description of the measures taken or proposed to be taken to address such event, including measures to mitigate its possible adverse effects.
- 6.4 Immediately following any unauthorised or unlawful Personal Data processing or Personal Data Breach, the parties will co-ordinate with each other to investigate the matter. Digital Shadows will reasonably co-operate with the Customer in the Customer's handling of the matter, including:
- 6.4.1 assisting with any investigation;
  - 6.4.2 making available all relevant records, logs, files, data reporting and other materials required to comply with all Data Protection Legislation or as otherwise reasonably required by the Customer; and
  - 6.4.3 taking reasonable and prompt steps to mitigate the effects and to minimise any damage resulting from the Personal Data Breach or unlawful Personal Data processing.
- 6.5 Digital Shadows will not inform any third party of any Personal Data Breach without first obtaining the Customer's prior written consent, except when required to do so by law, to maintain any policy of insurance, or to maintain regulatory or equivalent certifications.
- 6.6 Subject to clause 6.5 the Customer has the sole right to determine:
- 6.6.1 whether to provide notice of the Personal Data Breach to any Data Subjects, supervisory authorities, regulators, law enforcement agencies or others, as

**DIGITAL SHADOWS DATA PROCESSING TERMS**  
(Effective 25 November 2022)

required by law or regulation or in the Customer's discretion, including the contents and delivery method of the notice; and

- 6.6.2 whether to offer any type of remedy to affected Data Subjects, including the nature and extent of such remedy.

**7 CROSS-BORDER TRANSFERS OF PERSONAL DATA**

- 7.1 If an adequate protection measure for the international transfer of Personal Data is required under applicable data protection legislation (and has not otherwise been arranged by the parties) the Standard Contractual Clauses shall be incorporated into this DPA in the Schedules as if they had been set out in full.

- 7.2 The Customer consents to Digital Shadows (and its sub-Processors) transferring Personal Data outside the United Kingdom and the European Economic Area ("**GDPR Territories**"). Provided that where such processing occurs, Digital Shadows:

7.2.1 is processing Personal Data in a territory which is subject to a current finding by the European Commission under the Data Protection Legislation that the territory provides adequate protection for the privacy rights of individuals;

7.2.2 participates in a valid cross-border transfer mechanism under the Data Protection Legislation, so that Digital Shadows (and, where appropriate, the Customer) can ensure that appropriate safeguards are in place to ensure an adequate level of protection with respect to the privacy rights of individuals as required by Article 46 of the GDPR; or

7.2.3 otherwise ensures that the transfer complies with the Data Protection Legislation.

- 7.3 In the case of any Processing of Personal Data outside of the GDPR Territories as at the date of this DPA, Digital Shadows has identified in the Schedules the relevant transfer mechanism. Digital Shadows will promptly inform the Customer of any change to such mechanisms.

- 7.4 Where Customer's transfer of Personal Data to Digital Shadows (including in the context of an onward transfer) would be a transfer outside of the GDPR Territories under FADP, the EU Standard Contractual Clauses shall apply pursuant to clause 7.3, provided, however:

7.4.1 the term 'member state' shall not be interpreted in such a way as to exclude Data Subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c) of the EU Standard Contractual Clauses;

7.4.2 references to the GDPR should be understood as references to the FADP insofar as the data transfers are subject to the FADP;

7.4.3 the EU Standard Contractual Clauses also protects the data of legal entities until the entry into force of the revised FADP; and

7.4.4 the competent Supervisory Authority (for purposes of Annex 1.C (under Clause 13 of the EU Standard Contractual Clauses)) shall be the Federal Data Protection and Information Commissioner (FDPIC) insofar as the data transfer is governed by the FADP, and the EU authority specified in Annex 1.C insofar as the data transfer is governed by the GDPR.

- 7.5 The Customer authorises Digital Shadows to enter into the Standard Contractual Clauses with the sub-Processor on the Customer's behalf, if required to ensure the relevant Processing of Personal Data complies with Data Protection Legislation. Digital Shadows will make the executed Standard Contractual Clauses available to the Customer on written request.

- 7.6 To the extent Customer confirms that an actual transfer of Personal Data to Digital Shadows (including in the context of an onward transfer) is regulated by any jurisdiction's Data Protection Legislation other than GDPR, UK Data Protection legislation or FADP,

**DIGITAL SHADOWS DATA PROCESSING TERMS**  
(Effective 25 November 2022)

then Customer shall notify Digital Shadows of such actual transfer and the mandatory obligations under such jurisdiction's Data Protection Legislation, and the parties shall work together in good faith to determine if changes are needed to this DPA to accommodate such actual transfer and mandatory obligations.

**8 CALIFORNIA CONSUMERS**

- 8.1 The following terms apply to the extent Digital Shadows processes Personal Information about California consumers. These terms are in addition to all other requirements set forth in the DPA; provided, however, in the event of any conflict between these CCPA provisions and the remainder of this DPA, these CCPA provisions shall control with respect to personal information about California consumers.
- 8.2 The terms "consumer", "business", "personal information", "service provider", "business purpose", "commercial purpose", "sell" and "share" shall have the meanings defined under CCPA.
- 8.3 Customer and Digital Shadows acknowledge and agree that Customer is a business and Digital Shadows is a service provider.
- 8.4 Digital Shadows shall process Personal Information on behalf of Customer.
- 8.5 Digital Shadows shall not, in relation to any Personal Information for which Digital Shadows is a service provider:
- 8.5.1 sell or share Personal Information;
  - 8.5.2 retain, use, or disclose Personal Information for any purpose other than for the Service, including retaining, using, or disclosing Personal Information for a commercial purpose other than the Service, or as otherwise permitted under the CCPA, this DPA and the Agreement;
  - 8.5.3 retain, use, or disclose Personal Information outside of the direct business relationship between Digital Shadows and Customer; or
  - 8.5.4 combine the Personal Information it receives from, or on behalf of, Customer with personal information that it receives from, or on behalf of, another person or persons, or collects from its own interaction with the consumer, provided that Digital Shadows may combine personal information to perform any business purpose as permitted by the CCPA, this DPA and the Agreement.
- 8.6 If Digital Shadows engages any other person to assist it in processing Personal Information for the Service on behalf of Customer, or if any other person engaged by Digital Shadows engages another person to assist in processing Personal Information for the Service, Digital Shadows shall notify Customer of that engagement as set out at clause 9.1.

**9 SUB-PROCESSORS**

- 9.1 Digital Shadows may only authorise a third party (sub-Processor) to process the Personal Data if:
- 9.1.1 the Customer is provided with an opportunity to object to (but not prevent) the appointment of each sub-Processor within 10 days of Digital Shadows providing the Customer with reasonable details of the forthcoming changes to its sub-Processors, with such details to be provided by Digital Shadows updating its dedicated sub-Processor webpage at <https://info.digitalshadows.com/sub-processor.html>;
  - 9.1.2 Digital Shadows enters into a written contract with the sub-Processor that contains terms similar to those set out in this DPA, in particular, in relation to requiring appropriate technical and organisational data security measures, and, upon the Customer's written request and at the Customer's expense, provides

**DIGITAL SHADOWS DATA PROCESSING TERMS**  
(Effective 25 November 2022)

the Customer with copies of such contracts (subject to redaction of any confidential information); and

9.1.3 Digital Shadows maintains control over all Personal Data it entrusts to the sub-Processor.

9.2 The Customer authorises Digital Shadows to use sub-Processors set out on Digital Shadows' dedicated sub-Processor webpage at <https://info.digitalshadows.com/sub-processor.html>. These sub-processors include but are not limited to the general categories of data storage, hosting (including data centres and providers of virtual software environments) and IT support.

9.3 Where the sub-Processor fails to fulfil its obligations under such written agreement, Digital Shadows remains fully liable to the Customer for the sub-Processor's performance of its agreement obligations.

**10 COMPLAINTS, DATA SUBJECT REQUESTS AND THIRD-PARTY RIGHTS**

10.1 Digital Shadows will take such technical and organisational measures as may be appropriate, and promptly provide such information to the Customer as the Customer may reasonably require, to enable the Customer to comply with:

10.1.1 the rights of Data Subjects under the Data Protection Legislation, including subject access rights, the rights to rectify and erase Personal Data, object to the processing and automated processing of Personal Data, and restrict the processing of Personal Data; and

10.1.2 information or assessment notices served on the Customer by any supervisory authority under the Data Protection Legislation.

10.2 Digital Shadows will notify the Customer immediately if it receives any complaint, notice or communication that relates directly or indirectly to the processing of the Personal Data or to either party's compliance with the Data Protection Legislation.

10.3 Digital Shadows will notify the Customer without undue delay if it receives a request from a Data Subject for access to their Personal Data or to exercise any of their related rights under the Data Protection Legislation.

10.4 Digital Shadows will give the Customer its full co-operation and assistance in responding to any complaint, notice, communication or Data Subject request.

10.5 Digital Shadows will not disclose the Personal Data to any Data Subject or to a third party other than at the Customer's request or instruction, as provided for in this DPA or as required by law.

**11 LIABILITY**

11.1 Digital Shadows' total liability pursuant to this DPA shall be limited to the liability cap in the Agreement.

**12 TERM AND TERMINATION**

12.1 This DPA will remain in full force and effect so long as Digital Shadows retains any Customer Personal Data related to the Service in its possession or control.

12.2 Any provision of this DPA that expressly or by implication should come into or continue in force on or after termination of the Service in order to protect Personal Data will remain in full force and effect.

12.3 If a change in any Data Protection Legislation prevents either party from fulfilling all or part of the Service, the parties will discuss in good faith with a view to implementing any changes necessary to ensure the processing of Personal Data complies with the new requirements.

**DIGITAL SHADOWS DATA PROCESSING TERMS**  
(Effective 25 November 2022)

**13 DATA RETURN AND DESTRUCTION**

- 13.1 At the Customer's request, Digital Shadows will give the Customer a copy of or access to all or part of the Customer's Personal Data in its possession or control in a commonly accessible and electronic format determined by Digital Shadows.
- 13.2 On termination of the Service for any reason or expiry of its term, Digital Shadows will promptly securely delete or destroy or, if directed in writing by the Customer, return and not retain, all or any Personal Data related to this DPA in its possession or control. This requirement shall not apply to Personal Data which Digital Shadows has archived on its backup systems which are not reasonably accessible, provided that such Personal Data is deleted promptly in the event such backups become reasonably accessible (such as by Digital Shadows using those backups to restore its systems).
- 13.3 Clause 13.2 shall not apply to the extent any law, regulation, or government or regulatory body requires Digital Shadows to retain any documents or materials that Digital Shadows would otherwise be required to return or destroy.

**14 RECORDS**

- 14.1 Digital Shadows will keep detailed, accurate and up-to-date written records regarding any processing of Personal Data it carries out for the Customer ("**Records**") and provide the Customer with copies of the Records upon request.

**15 AUDIT**

- 15.1 No more than once during any consecutive 12 month period, on request from the Customer Digital Shadows will provide the Customer with the relevant information from its ISO 27001:2013 audit (which may have been carried out internally or by third-party representatives) to evidence its compliance with this DPA and provide the summary results to the Customer. The Customer shall be entitled to ask questions of Digital Shadows related to compliance with Data Protection Legislation in advance of the audit, Digital Shadows shall use its reasonable endeavours to respond adequately when providing the audit results.
- 15.2 On the Customer's written request, Digital Shadows will exercise relevant audit rights it has in connection with its sub-Processors' compliance with their obligations regarding the Customer's Personal Data, and provide the Customer with a summary of the audit results.
- 15.3 The audit rights set out at clauses 15.1 – 15.2 are the Customer's only contractual rights (and Digital Shadows' only contractual obligations) in connection with the auditing of Digital Shadows' Processing of Personal Data. Save that nothing in this DPA shall prevent or is intended to undermine the rights and powers granted to Data Subjects or Supervisory Authorities, and accordingly Digital Shadows shall submit to any audits required by a Supervisory Authority or Data Protection Legislation.



**DIGITAL SHADOWS DATA PROCESSING TERMS**  
(Effective 25 November 2022)

**SCHEDULE 1**

**EU TO THIRD COUNTRY TRANSFERS**

**1 INCORPORATION OF THE EU STANDARD CONTRACTUAL CLAUSES**

1.1 To the extent clause 7.1 applies and the transfer is made pursuant to the GDPR, this Schedule 1 and the following terms shall apply: Module 2 of the EU Standard Contractual Clauses, and no other optional clauses unless explicitly specified, are incorporated into this Schedule 1 as if they had been set out in full in the case where the exporter is a Controller, the importer is a Processor and the transfer requires such additional protection.

**2 CLARIFICATIONS TO THE EU STANDARD CONTRACTUAL CLAUSES**

2.1 Deletion of data. For the purposes of clause 8.5 of the EU Standard Contractual Clauses (Duration of processing and erasure or return of data), the parties agree as follows: At the end of the provision of the Processing services the data importer shall delete all Personal Data and shall certify to the data exporter that it has done so, if requested to provide such certification by the data exporter in writing.

2.2 Auditing. The parties acknowledge that the data importer complies with its obligations under clause 8.9 of the EU Standard Contractual Clauses (Section II to the Standard Contractual Clauses (Documentation and compliance)) by exercising its contractual audit rights it has agreed with its sub-processors.

2.3 Sub-Processors. For the purposes of clause 9 of the EU Standard Contractual Clauses (Section II to the Standard Contractual Clauses (Use of sub-processors)), the parties agree that the data importer can use the sub-processors set out at clause 9.2.

2.4 International Transfer Assessments. For the purposes of clause 14(c) of the EU Standard Contractual Clauses (Local laws and practices affecting compliance with the Clauses)) the data exporter has been provided with a transfer impact assessment by the data importer which the data exporter accepts as sufficient to fulfil the data importer's obligations pursuant to clause 14(c) and 14(a). The data exporter acknowledges that it has been provided with the security measures applied to the Personal Data and approves such measures as being in compliance with the EU Standard Contractual Clauses.

2.5 Best Efforts Obligations. For the purposes of clauses 14(c), 15.1(b) and 15.2 of the EU Standard Contractual Clauses (Section III to the Standard Contractual Clauses (Local laws and practices affecting compliance with the Clauses)) the parties agree that "best efforts" and the obligations of the data importer under clause 15.2 shall mean exercising the degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a leading practice engaged in a similar type of undertaking under the same or similar circumstances and shall not include actions that would result in civil or criminal penalty such as contempt of court under the laws of the relevant jurisdiction.

2.6 Competent Supervisory Authority. For the purposes of clause 13 of the EU Standard Contractual Clauses, the Competent Supervisory Authority shall be:

2.6.1 If the data exporter is established in the EU: The Irish Data Protection Commissioner.

2.6.2 Where the data exporter is not established in an EU Member State and has appointed a representative pursuant to Article 27(1) regulation (EU) 2016/679, it shall notify Digital Shadows of this and the EU Member State in which the exporter's representative is appointed shall be the competent supervisory authority.

**DIGITAL SHADOWS DATA PROCESSING TERMS**  
(Effective 25 November 2022)

2.6.3 Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) but has not appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: the data exporter shall notify Digital Shadows of its chosen competent supervisory authority, which must be the supervisory authority of a Member State in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located.

2.7 Governing Law & Jurisdiction. For the purposes of clauses 17 and 18 of the EU Standard Contractual Clauses, the parties agree that the governing law shall be where the data exporter is established. If those laws do not allow for 3rd party rights, the law of Ireland shall apply.

### **3 APPENDICES AND ANNEXURES TO THE STANDARD CONTRACTUAL CLAUSES**

The processing details required by the EU Standard Contractual Clauses are set out in paragraph 4:

3.1 the details required at Annex 1.A of the EU Standard Contractual Clauses is set out at paragraphs 4.1 – 4.2;

3.2 the details required at Annex 1.B of the EU Standard Contractual Clauses is set out at paragraph 4.3 – 4.10; and

3.3 the details required at Annex 1.C of the EU Standard Contractual Clauses is set out a paragraph 4.11; and

3.4 the details required at Annex 2 of the EU Standard Contractual Clauses is set out at paragraph 4.12.

### **4 PROCESSING PARTICULARS FOR THE STANDARD CONTRACTUAL CLAUSES**

#### The Parties

4.1 **Exporter (Controller):** The Customer

4.2 **Importer (Processor):** Digital Shadows

#### Description Of Data Processing

4.3 **Categories of data subjects:** Key individuals employed by the Customer, the Customer's customers and other key individuals working with or for the Customer in a consultancy capacity.

4.4 **Categories of personal data transferred:** Names, work and home addresses, email addresses, contact details, aliases and social media accounts

4.5 **Sensitive data transferred:** Not applicable.

4.6 **Frequency of the transfer:** One main transfer at the outset of the agreement, followed by smaller, continuous transfers.

4.7 **Nature of the processing:** Personal data will be used by Digital Shadows to identify potential data breaches and security vulnerabilities, principally by assessing the bank of data held by Digital Shadows against the relevant Personal Data.

4.8 **Purpose of the processing:** The provision of the SearchLight Services.

4.9 **Duration of the processing:** For the duration of the DPA (and subject to Digital Shadows' backup and retention policy).

4.10 **Sub-Processor Transfers:** As set out at clause 9

4.11 **Competent Supervisory Authority:** As set out at paragraph 2.6.

4.12 **Technical and Organisational Measures:** As set out at Annex 1.

**DIGITAL SHADOWS DATA PROCESSING TERMS**  
(Effective 25 November 2022)

**SCHEDULE 2**

**UK INTERNATIONAL TRANSFER ADDENDUM TO THE EU STANDARD CONTRACTUAL CLAUSES (the "Addendum")**

To the extent there is a transfer of Personal Data between the Parties which requires additional protection under the UK GDPR, this Schedule 2 and the following terms shall apply: the template addendum issued by the Information Commissioner's Office and laid before Parliament in accordance with s119A of the DPA 2018 on 2 February 2022 is incorporated into this Schedule 2 as if it had been set out in full in (where the exporter is a controller, the importer is a controller and the Parties have not otherwise arranged such additional protection).

**1. Parties**

As set out in Schedule 1.

**2. Selected SCCs, Modules and Clauses**

Module 2 of the EU Standard Contractual Clauses and no other optional clauses unless explicitly specified, and as amended by the clarifications in Schedule 1, paragraph 2.

**3. Appendix Information**

The processing details required by the Addendum are as set out in Schedule 1, paragraph 4.

**4. Termination of the UK Addendum**

In the event the template Addendum is amended, either party may terminate this Schedule 2 on written notice to the other in accordance with Table 4 and paragraph 19 of the Addendum and replace it with a mutually acceptable alternative.

**DIGITAL SHADOWS DATA PROCESSING TERMS**  
(Effective 25 November 2022)

**ANNEX 1**

**SECURITY MEASURES IMPLEMENTED BY THE DATA IMPORTER**

Digital Shadows has created an Information Security Management System (ISMS) designed and certified to the international standard ISO 27001:2013.

Contained within the ISMS is an Information Security Policy Statement, which is signed by the company founders (CEO and CIO).

The policy statements are designed against best practice and they describe disaster recovery, protective marking, incident management, privacy, data retention and destruction and laptop security.

These policies are included in the staff on-boarding and are available on the company intranet.

The ISMS sets out a governance process for maintaining, creating and approving policies.

The ISMS also regularly reviews policies and updates them as required.

All code used in the Services are developed against the Open Web Application Security Project (OWASP) standards.

Customer data is logically separated throughout the Service at the presentation, application and database layers.

Strong identity and access controls are implemented that use two-factor authentication being required to access the client facing web application.

All data at rest or in-transit is encrypted.

Vulnerability assessments are performed quarterly. Penetration tests of the applications and Digital Shadows infrastructure are conducted by CREST approved vendors are performed annually.

Digital Shadows also perform internal purple team exercises regularly.

Access to Digital Shadows' environment is controlled by the principle of least privilege.

Digital Shadows' hosting provider has additional security safeguards for Denial of Service, Firewalls, network intrusion detection (NIDS) Logs are sent to Digital Shadows SIEM (security incident and event management) system.

This Security Incident and Event Management system is monitored 24/7 by Digital Shadows' managed security service provider (MSSP).